

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА БІОМЕДИЧНОЇ ІНЖЕНЕРІЇ ТА ТЕЛЕКОМУНІКАЦІЙ

УДК 654.9:004.891

«Допущено до захисту»

Завідувач кафедри біомедичної
інженерії та телекомунікацій
к.т.н., доц. Нікітчук Т.М.

«14» грудня 2021 р.

КВАЛІФІКАЦІЙНА РОБОТА

на тему Дослідження інженерно-програмного комплексу технічних засобів
системи безпеки об'єкта

за спеціальністю 172 «Телекомунікації та радіотехніка»
освітній ступінь «магістр»

Виконавець роботи
студент 2 курсу, гр.ЗТРм-20-1

10.12.2021
(дата, підпис)

Фурман С.В.

Керівник роботи
к.т.н., доц.

10.12.2021
(дата, підпис)

Дубина О.Ф.

Житомир
2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»
ФАКУЛЬТЕТ ІНФОРМАЦІЙНО-КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ
КАФЕДРА БІОМЕДИЧНОЇ ІНЖЕНЕРІЇ ТА ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка
до кваліфікаційної магістерської роботи

на тему Дослідження інженерно-програмного комплексу технічних засобів
системи безпеки об'єкта

Виконав: студент 2 курсу,
групи ЗТРм-20-1 спеціальності
172 «Телекомунікації та радіотехніка»

Фурман С.В.

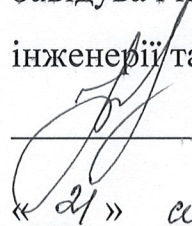
Керівник Дубина О.Ф.

Рецензент Нікітчук Т.М.

Житомир
2021

«Затверджено»

Завідувач кафедри біомедичної
інженерії та телекомунікацій

 Т.М. Нікітчук

«21» січня 2021 р.

Завдання на кваліфікаційну магістерську роботу

Фурман Сергій В'ячеславович
(прізвище, ім'я, по батькові)

1. Тема роботи Дослідження інженерно-програмного комплексу технічних засобів системи безпеки об'єкта затверджено наказом по університету від «08» 11 2021 р. № 547/с
2. Мета дослідження: дослідження особливостей функціонування інтегрованого апаратно-програмного комплексу системи безпеки об'єкту та можливості проведення тематичної обробки зображень системи відеоспостереження для забезпечення виконання завдань.
3. Вихідні дані (характеристики об'єкта, умов дослідження та ін. Інженерно-програмний комплекс технічних засобів системи безпеки об'єкту. Параметри дослідження системи відеоспостереження – кут поля зору та роздільна здатність на місцевості
4. Основні задачі дослідження: проаналізувати комплексні системи безпеки об'єктів, провести аналіз ІКБ, дослідити можливості ІКБ та залежність якості обробки зображень системи відеоспостереження та відеоаналізу від кута поля зору та роздільної здатності відеокамер.

5. Термін подання роботи до захисту грудень 2021 р.

6. Дата видачі завдання «21» 01 2021 р.

Науковий керівник

Завдання прийняв
до виконання

(підпис)

(підпис)

(прізвище, ініціали)

(прізвище, ініціали)

Дубина О.Ф.

Фурман С.В.

АНОТАЦІЯ

Темою дипломної роботи є інженерно-програмного комплексу технічних засобів систем безпеки об'єкта. Проведено аналіз комплексних систем безпеки спеціальних об'єктів. Розкрито принципи організації, структуру, склад, принцип дії інтегрованих систем безпеки. Проведено аналіз інженерно-програмного комплексу технічних засобів систем безпеки об'єкту. Показано три основні складові комплексу: система контролю доступу, система охоронної сигналізації. Система відеоспостереження та відеоконтролю. Проведено дослідження можливостей роботи програмно-апаратного комплексу побудови ІКБ, платформи ІКБ та програмного забезпечення. Для забезпечення можливості тематичної обробки зображень в цілях охорони об'єктів було проведено дослідження параметрів системи відеоспостереження та відеоконтролю по таким параметрам, як кут поля зору, роздільна здатність відеокамери для забезпечення можливості виявлення, розпізнавання та ідентифікації об'єктів на зображеннях.

Результати проведених досліджень можуть використовуватися під час проектування інтегрованої системи охорони об'єктів.

ANNOTATION

The topic of the thesis is the engineering and software complex of technical means of security systems of the object. The analysis of complex security systems of special objects is carried out. The principles of organization, structure, composition, principle of operation of integrated security systems are revealed. The analysis of the engineering and software complex of technical means of security systems of the object is carried out. Three main components of the complex are shown: access control system, burglar alarm system. Video surveillance and video surveillance system. A study of the possibilities of the software and hardware complex for the construction of the ICB, the ICB platform and software. To enable thematic image processing for the protection of objects, a study of the parameters of the video surveillance and video

surveillance system on such parameters as the angle of view, the resolution of the video camera to enable detection, recognition and identification of objects in images.

The results of the research can be used in the design of an integrated security system.

РЕФЕРАТ

Дипломна робота має на меті дослідження особливостей функціонування інтегрованого апаратно-програмного комплексу системи безпеки об'єкту та можливості проведення тематичної обробки зображень системи відеоспостереження для забезпечення виконання завдань.

Дана дипломна робота містить: сторінок – 89, таблиць – 1, рисунків – 24.

У першому розділі проведено аналіз комплексних систем безпеки спеціальних об'єктів. Розкрито принципи організації, структуру, склад, принцип дії інтегрованих систем безпеки. Показано, що тільки комплексна система охорони у складі систем відеоспостереження, охоронної та пожежної сигналізації, контролю управління доступу може забезпечити виконання завдань безпеки з необхідними показниками.

У другому розділі проведено аналіз інженерно-програмного комплексу технічних засобів систем безпеки об'єкту. Показано три основні складові комплексу: система контролю доступу, система охоронної сигналізації. Система відеоспостереження та відеоконтролю. Розкрито їх основні проектні рішення та принципи та порядок функціонування.

У третьому розділі проведено дослідження інтегрованого апаратно-програмного комплексу безпеки об'єкту. Проведено дослідження можливостей роботи програмно-апаратного комплексу побудови ІКБ, платформи ІКБ та програмного забезпечення. Для забезпечення можливості тематичної обробки зображень в цілях охорони об'єктів було проведено дослідження параметрів системи відеоспостереження та відеоконтролю по таким параметрам, як кут поля зору, роздільна здатність відеокамери для забезпечення можливості виявлення, розпізнавання та ідентифікації об'єктів на зображеннях.

Ключові слова: інтегрована система охорона, система охоронної сигналізації, система відеоспостереження та відеоаналізу, відеокамера, датчик, відеосервер, роздільна здатність, кут поля зору.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ.....	9
ВСТУП.....	11
РОЗДІЛ 1 АНАЛІЗ КОМПЛЕКСНИХ СИСТЕМ БЕЗПЕКИ СПЕЦІАЛЬНИХ ОБ'ЄКТІВ.....	12
1.1 Визначення та класифікація охоронних систем.....	12
1.2 Структура комплексної системи безпеки.....	13
1.3 Призначення та класифікація технічних засобів охорони об'єктів.....	15
РОЗДІЛ 2 АНАЛІЗ ІНЖЕНЕРНО-ПРОГРАМНОГО КОМПЛЕКСУ ТЕХНІЧНИХ ЗАСОБІВ СИСТЕМ БЕЗПЕКИ ОБ'ЄКТУ.....	37
2.1 Система контролю доступу.....	37
2.1.1 Основні проектні рішення СКД.....	37
2.1.2 Конфігурація системи СКД.....	39
2.1.3 Функціонування системи СКД.....	39
2.2 Система охоронної сигналізації.....	40
2.2.1 Основні проектні рішення СОС.....	40
2.2.2 Конфігурація системи СОС.....	41
2.3.3 Функціонування системи СОС.....	41
2.3 Система відеоспостереження та відеоконтролю	42
2.3.1 Основні проектні рішення СВН.....	42
2.3.2 Конфігурація системи СВН.....	43
2.3.3 Функціонування системи СВН.....	44
РОЗДІЛ 3 ДОСЛІДЖЕННЯ ІНТЕГРОВАНОГО АПАРАТНО- ПРОГРАМНОГО КОМПЛЕКСУ БЕЗПЕКИ ОБ'ЄКТУ.....	50
3.1 Дослідження можливостей роботи програмно-апаратного комплексу побудови ІКБ	50
3.2 Дослідження можливостей і характеристик платформи ІКБ та програмного забезпечення.....	51

3.3 Дослідження програмного забезпечення для відеоспостереження та сервісної відеоаналітики.....	52
3.4 Дослідження лінгвістичного забезпечення	55
3.5 Дослідження механізму автоматизованого контролю, аналізу інформації моніторингу, прогнозування ситуацій з масовим перебуванням людей.....	56
3.6 Дослідження параметрів системи відеоспостереження та відеоконтролю.....	57
3.6.1 Дослідження кута поля зору відеокамер	57
3.6.2 Дослідження можливостей тематичної обробки зображень відеокамер.....	61
ВИСНОВОК.....	70
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	71
ДОДАТОК	73

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СОС – система охоронної сигналізації;

СВН – система відеоспостереження та відеоконтролю;

ППК – прилад приймально-контрольний;

АРМ – автоматизоване робоче місце;

ПЗ – програмне забезпечення;

ІКБ – інтегрований комплекс безпеки.

ІЧ-сенсор – сенсор з чутливим елементом, що реагує на інфрачервоне випромінювання;

НВО – науково виробничого об'єднання;

AAC – Advanced Audio Coding;

AVI – Audio Video Interleave;

BNC – Bayonet Neill-Concelman;

DVR – Digital Video Recorder;

G.711 – Рекомендація

ITU-T – міжнародний стандарт для модуляції мовних сигналів;

G.726 – Кодек є стандартом ITU-T адаптивної імпульсно-кодової модуляції;

GSM – Global System for Mobile Communications

HDMI – High Definition Multimedia Interface

H.264 – Advanced Video Coding;

MJPEG – Motion JPEG – покадровий метод видеосжатия;

MPEG-4 – Moving Picture Experts Group;

PCM – Pulse Code Modulation;

Pelco-D – Протокол управління камерою, що використовується в галузі відеоспостереження;

Pelco-P – Протокол управління камерою, що використовується в галузі відеоспостереження;

PTZ-камера – Pan / Tilt / Zoom камера;

RS-485 – Recommended Standard 485;

RS-232 – Recommended Standard 232;

TCP/IP – Transmission Control Protocol/Internet Protocol

VGA – Video Graphics Array;

Wi-Fi – Wireless Fidelity.

ВСТУП

У теперішній час забезпечення власної безпеки, а також охорони нерухомої власності стало необхідністю. Рішення цього можливе тільки при грамотному оснащенні систем безпеки сучасними високонадійними технічними засобами системи охорони. Клієнтами охоронних компаній стають все більше приватних підприємств, організацій, транспортних засобів та навіть об'єкти у держаній власності. Попит на сучасні та високонадійні системи безпеки зростає, тому компанії виробники таких систем постійно знаходяться у атмосфері жорсткої конкуренції, що забезпечує стрімкий технічний розвиток. Тому дослідження інженерно-програмного комплексу технічних засобів систем безпеки об'єкта вважаю актуальною темою магістерської роботи.

Метою роботи є дослідження особливостей функціонування інтегрованого апаратно-програмного комплексу системи безпеки об'єкту та можливості проведення тематичної обробки зображень системи відеоспостереження для забезпечення виконання завдань.

Для досягнення мети були поставлені такі завдання:

1. Провести аналіз комплексних систем безпеки спеціальних об'єктів.
2. Провести аналіз інженерно-програмного комплексу технічних засобів систем безпеки об'єкту
3. Провести дослідження інтегрованого апаратно-програмного комплексу безпеки об'єкту.

Об'єктом дослідження є технічна система охорони об'єкту.

Предметом дослідження є інтегрований апаратно-програмний комплекс системи безпеки об'єкту.

Практична цінність отриманих результатів полягає у надання пропозицій для вибору відеокамер з необхідними параметрами і характеристиками у залежності від геометричних параметрів об'єкта, що охороняється і завдань, що необхідно виконувати.

1 АНАЛІЗ ІНТЕГРОВАНИХ СИСТЕМ БЕЗПЕКИ СПЕЦІАЛЬНИХ ОБ'ЄКТІВ

1.1 Визначення та класифікація систем охорони

Система безпеки –комплекс для охорони різних об'єктів, таких як будівля, включаючи прилеглу територію, окремі приміщення, автомобілі, водний транспорт та ін. Головне призначення охоронної системи - унеможливлення несанкціонованого проникнення в приміщення, що знаходиться під охороною та оперативне і гарантоване сповіщення власників і правоохоронних служб про спробу здійснення незаконних дій щодо майна в приміщенні або самого об'єкту що охороняється. Крім того, можливість розпізнати злочинців з записів відеоспостереження або навіть затримати на місці злочину за допомогою активних систем безпеки. Система безпеки - узагальнюючий термін для декількох типів систем, а саме: контролю доступу, охоронної та пожежної сигналізації, відеоспостереження.

Класифікація систем безпеки приміщень.

За взаємодією із загрозою:

- Пасивні – під час спрацювання власник або служби охорони отримують сповіщення про проникнення в приміщення;
- Автономна охоронна система – засоби, що діють локально привертаючи увагу звуком та світловими ефектами.
- Централізована пультова сигналізація – при спрацьовуванні такої сигналізації на об'єкт вирушає оперативна група охорони.

За способом передачі інформації:

- Дротові – лінії витої пари, оптиковолоконні та телефонні;
- Бездротові — в них охоронні сенсори надсилають інформацію на приймальний засіб за допомогою радіохвиль по просторі.

1.2 Структура інтегрованої системи безпеки

Реалізація концепції безпеки передбачає декілька напрямків забезпечення захищеності об'єкта – це економічна, технологічна, екологічна, інформаційна, інженерно-технічна безпека. Всі вони є елементами єдиної системи інтегрованої безпеки даного об'єкту. До складу комплексу технічних засобів забезпечення безпеки об'єкту повинні входити наступні технічні підсистеми [6, 10, 13]:

- охоронної та пожежної сигналізації;
- контролю та управління доступом;
- відеоспостереження;
- пошуку і огляду;
- пожежної автоматики;
- оповіщення та управління евакуацією;
- засоби зв'язку з об'єктом;
- захисту інформації;
- інженерного забезпечення об'єкта.

Склад і кількість об'єктових підсистем безпеки можуть змінюватися залежно від призначення об'єкта, що захищається і певних умов з комплексного забезпечення його безпеки.

Таким чином, будемо розглядати задачу забезпечення захисту об'єкта силами чотирьох основних нероздільних підсистем комплексу технічних засобів забезпечення безпеки, окремо виконують свої функції: системи охоронної і пожежної сигналізації, системи контролю та управління доступом, системи відеоспостереження. Комплекс доповнюють різні допоміжні пристрої, наприклад, системи електроживлення, освітлення, оповіщення, запобігання і ліквідації загроз і інші системи, які забезпечують життєздатність і надійне функціонування основних підсистем. Кожна з основних підсистем може розглядатися як інтегрована системи безпеки, яка відпрацьовує свій комплекс загроз і включає в себе сукупність технічних засобів охорони.

Технічні засоби охорони (ТЗО) є основним поняттям, що позначає апаратуру, яка використовується в складі комплексів забезпечення безпеки

об'єктів від несанкціонованого проникнення. Структура інтегрованої системи безпеки виконується за класичною схемою і складається з наступних елементів [2, 10]:

- СЗОІУЦ (система збору та обробки інформації та управління центральна)
- сервер, де зберігаються і обробляються усі бази даних системи; контрольні панелі, пульти, консолі управління;
- СЗОІУП (система збору та обробки інформації та управління периферійна);
- пристрої (контролери, розширювачі, пульти управління), безпосередньо на апаратному рівні взаємодіючі зі своїми сенсорами, сенсорами або виконавчими пристроями, а на інформаційному рівні зв'язують їх ПЗ локальному інтерфейсу (RS-485, RS-232) з робочими станціями або зі сервером;
- ЗВЗ (засоби виявлення загроз) – сенсори тривожної, охоронної, пожежної сигналізації, клавіатури, зчитувачі, відеокамери;
- СПП (система передачі повідомлень) – канали і засоби передачі тривожних та службових сповіщень, візуальної та акустичної інформації про об'єкт і стан системи безпеки;
- ЛКМ (локальна комп'ютерна мережа) – інформаційно і логічно зв'язує в єдиний комплекс окремі компоненти системи;
- ПЗ – системне, мережеве і прикладне програмне забезпечення сервера і робочих станцій, а також вбудоване програмне забезпечення системних контролерів, контрольних панелей і модулів;
- СБЖ (система безперебійного електроживлення);
- ДП – допоміжні пристрої, які забезпечують виконання системою охорони ряду інших функцій і включають в себе:
 - ЗО – засоби оповіщення;
 - ЗВІ – засоби відображення інформації;
 - ЗРД – засоби реєстрації даних;
 - ЗПЛЗ – засоби протидії та ліквідації загроз.

Узагальнена структурна схема інтегрованої системи безпеки приведена на рис. 2.1.

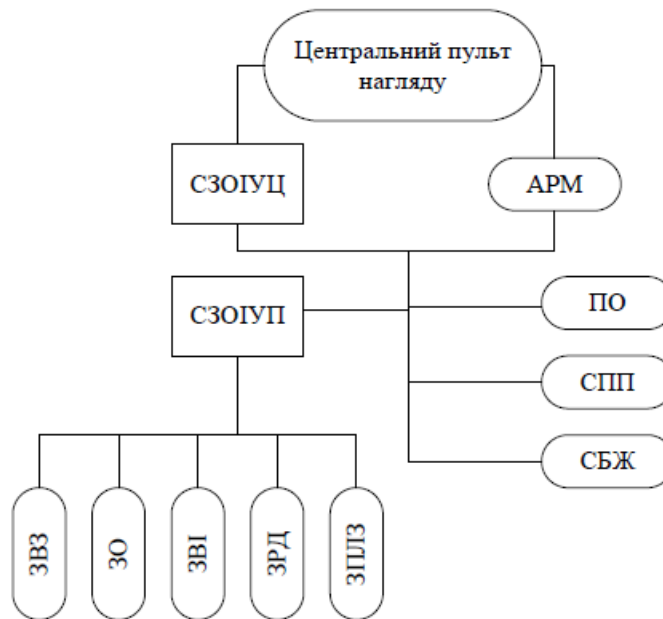


Рисунок 2.1 – Узагальнена структурна схема інтегрованої системи безпеки

З огляду на важливість кожного елемента узагальненої структурної схеми, необхідно виділити три основні групи ТЗО, без яких практично неможлива реалізація системи безпеки: пристрої виявлення загроз на об'єкті, система збору та обробки інформації і система управління, а також засоби передачі інформації про стан системи, доведення її до споживача (користувачів системи, спеціальних служб і т.д.). Перераховані засоби забезпечують вчасну та адекватну реакцію інтегрованої системи безпеки на виявлену подію.

1.3 Призначення та класифікація технічних засобів охорони об'єктів

Система охоронної сигналізації є комплексом технічних засобів, службовців для своєчасного виявлення небезпеки у приміщеннях, на об'єктах [1].

До технічних засобів охорони належать:

- системи охоронної та пожежної сигналізації;
- системи контролю і управління доступу;
- системи відеоспостереження;

- комплекси, з урахуванням ЕОМ, які включають перелічені системи.

Наведені вище системи можуть працювати як у комплексі, так і окремо. Наприклад, охорона та відеоспостереження може здійснюватися за великою кількістю об'єктів або однією квартирою чи офісом.

Системи будь-якої складності будуються на базі тих самих технічних пристроїв. При вирішенні технічних завдань охорони насамперед необхідно вибрати основні параметри пристроїв, які забезпечать достатню надійність виконання покладених на них функцій.

Системи охоронної сигналізації фіксують факт несанкціонованого доступу на територію, що охороняється, передають сигнал тривоги, наприклад, на пульт охорони і включають виконуючі пристрої.

Основні вимоги до технічних засобів охорони.

Технічними засобами охорони повинні бути обладнані всі приміщення з постійним або тимчасовим зберіганням матеріальних та інших цінностей, а також суміжні приміщення та вразливі місця (вікна, двері, люки, вентиляційні шахти та короби), розташовані на першому та останньому поверхах будівлі по периметру об'єкта [3,7].

Об'єкти підгруп БІ рекомендується обладнати однорубіжною охороною, підгруп АІ та БІІ – багаторубіжною охороною. У приміщеннях об'єктів підгрупи БІ, розташованих на другому та вище поверсі, а також усередині об'єкта, що охороняються по всьому периметру, встановлювати технічні засоби охорони не потрібно.

Допускається не обладнати технічними засобами охорони віконні отвори приміщень об'єктів підгруп АІ та БІІ, розташовані на другому та вище поверсі будівлі, що охороняється по всьому периметру.

Першим кордоном охорони мають бути захищені:

- віконні та дверні прорізи по периметру будівлі або будівлі об'єкта;
- місця введення комунікацій, вентиляційні канали;
- виходи до пожежних драбин;
- некапітальні та капітальні (якщо необхідний їх захист) стіни.

Допускається замість блокування засклених конструкцій на «відкриття» та «руйнування», внутрішніх некапітальних стін на «брухт», дверей на «відкриття» та «брухт» здійснювати блокування зазначених конструкцій тільки на «проникнення» за допомогою об'ємних та лінійних сповіщувачів. При цьому слід мати на увазі, що пасивні оптико-електронні сповіщувачі забезпечують захист приміщення тільки від безпосереднього проникнення порушника.

Блокування будівельних конструкцій на «відчинення» (двері, засклені конструкції) рекомендується здійснювати магнітоконттактними сповіщувачами, а блокування воріт, вантажно-розвантажувальних люків, дверей сховищ, ліфтових шахт - кінцевими вимикачами.

Блокування засклених конструкцій на «руйнування» скла рекомендується здійснювати сповіщувачами лінійними електроконтактними (фольга) або поверхневими сповіщувачами ударно-контактними. Блокування стін на пролом слід здійснювати сповіщувачами поверхневими п'єзоелектричними або сповіщувачами лінійними електроконтактними (провід типу НВМ).

Другим кордоном охорони повинен бути захищений обсяг приміщення за допомогою пасивних оптико-електронних сповіщувачів з об'ємною зоною виявлення, ультразвуковими, радіохвильовими або комбінованими сповіщувачами.

Третім кордоном охорони повинні бути захищені сейфи та окремі предмети або підходи до них за допомогою ємнісних, вібраційних, пасивних та активних оптико-електронних або радіохвильових сповіщувачів.

Вибір технічних засобів охорони та їх розміщення у приміщенні об'єкту.

У приміщенні об'єкта слід встановлювати такі технічні засоби охорони, щоб, з одного боку, забезпечувався необхідний рівень надійності охорони об'єкта, з іншого - скоротили б витрати (по можливості) на їх придбання, монтаж та експлуатацію.

Ступінь впливу перешкод на роботу технічних засобів охоронної та тривожної сигналізації залежить від їх потужності та принципу дії, а також схемно-технічних рішень апаратури.

Технічні засоби охоронної сигналізації.

Система охоронної сигналізації: сукупність спільно діючих технічних засобів виявлення проникнення (спроби проникнення) на об'єкт, що охороняється, збору, обробки, передачі та подання в заданому вигляді інформації про проникнення (спроби проникнення) та іншої службової інформації.

Система охоронної сигналізації у складі охоронно-пожежної сигналізації виконує завдання своєчасного оповіщення служби охорони про факт несанкціонованого проникнення або спробу проникнення людей у будівлю або окремі приміщення з фіксацією дати, місця та часу порушення рубежу охорони [3, 8].

Комплекс заходів охорони об'єкта:

- 1) створення шляху порушника фізичних перешкод;
- 2) раннє виявлення зловмисника (на далеких підступах до мети його руху);
- 3) оцінку ситуації;
- 4) вживання негайних заходів щодо припинення дій зловмисника;
- 5) відеодокументування;
- 6) передача сигналів тривоги чи повідомлень про подію.

Обладнання приміщень об'єкта технічними засобами охоронної сигналізації провадиться після проведення робіт з інженерно-технічної укріпленості.

На об'єкті, що охороняється чи передається під охорону приватним охоронним підприємством, слід встановлювати технічні засоби охоронної сигналізації, рекомендовані до застосування позавідомчою охороною.

Для підвищення надійності охорони об'єкта та його приміщень визначається структура системи охоронної сигналізації залежно від:

- режим роботи об'єкта;
- порядку проведення операцій із цінностями;
- особливостей розташування приміщень із цінностями всередині будівлі;

- вибору кількості зон, що охороняються, рубежів охорони, ШС. Основні вимоги до технічних засобів охоронної сигналізації:

Технічними засобами охоронної сигналізації повинні бути обладнані всі приміщення з постійним або тимчасовим зберіганням матеріальних та інших цінностей, а також суміжні приміщення та вразливі місця (вікна, двері, люки, вентиляційні шахти та короби), розташовані на першому та останньому поверхах будівлі по периметру об'єкта.

Об'єкти підгруп БІ рекомендується обладнати однорубежною охороною, підгруп АІ та БІІ – багаторубежною охороною.

У приміщеннях об'єктів підгрупи БІ, розташованих на другому та вище поверсі, а також усередині об'єкта, що охороняються по всьому периметру, встановлювати технічні засоби охоронної та тривожної сигналізації не потрібно.

Допускається не обладнати технічними засобами охоронної та тривожної сигналізації віконні отвори приміщень об'єктів підгруп АІ та БІІ, розташовані на другому та вище поверсі будівлі, що охороняється по всьому периметру.

Першим рубежем охорони повинні бути захищені: віконні та дверні прорізи по периметру будівлі або будови об'єкта; місця введення комунікацій; вентиляційні канали; виходи до пожежних драбин; некапітальні та капітальні (якщо необхідний їх захист) стіни.

Дверні прорізи, вантажно-розвантажувальні люки блокують на «відкриття» та «брухт» (тільки для дерев'яних).

Засклені конструкції блокують на «відкриття» та «руйнування» скла.

Місця введення комунікацій, некапітальні та капітальні стіни (якщо це необхідно) блокують на пролом.

Вентиляційні короби, димарі блокують на «руйнування».

Допускається замість блокування засклених конструкцій на «відкриття» та «руйнування», внутрішніх некапітальних стін на «брухт», дверей на «відкриття» та «брухт» здійснювати блокування зазначених конструкцій тільки на «проникнення» за допомогою об'ємних та лінійних сповіщувачів. При цьому слід мати на увазі, що пасивні оптико-електронні сповіщувачі («Фотон» та інші

аналогічні сповіщувачі), забезпечують захист приміщення тільки від безпосереднього проникнення порушника.

Блокування будівельних конструкцій на «відчинення» (двері, засклені конструкції) рекомендується здійснювати магнітоконтakтними сповіщувачами, а блокування воріт, вантажно-розвантажувальних люків, дверей сховищ, ліфтових шахт - кінцевими вимикачами.

Блокування засклених конструкцій на руйнування скла рекомендується здійснювати сповіщувачами лінійними електроконтактними (фольга) або сповіщувачами поверхневими ударно-контактними.

Блокування стін на пролом слід здійснювати сповіщувачами поверхневими п'єзоелектричними або сповіщувачами лінійними електроконтактними (провід типу НВМ).ним кордоном охорони повинен бути захищений обсяг приміщення за допомогою пасивних оптико-електронних сповіщувачів з об'ємною зоною виявлення, ультразвуковими, радіохвильовими або комбінованими сповіщувачами.

Третім кордоном охорони повинні бути захищені сейфи та окремі предмети або підходи до них за допомогою ємнісних, вібраційних, пасивних та активних оптико-електронних або радіохвильових сповіщувачів.

Вибір технічних засобів охоронної сигналізації та їх розміщення у приміщенні об'єкту.

У приміщенні об'єкта слід встановлювати такі технічні засоби охоронної сигналізації, щоб, з одного боку, забезпечувався необхідний рівень надійності охорони об'єкта, з іншого - скоротили б витрати (по можливості) на їх придбання, монтаж та експлуатацію.

Вибір конкретного типу сповіщувача визначається залежно від:

- зіставлення конструктивних будівельних показників об'єкта, що підлягає захисту, і тактико-технічних параметрів сповіщувача;
- характеру та розміщення цінностей у приміщеннях;
- Поверховості будівлі;
- завадової обстановки на об'єкті;

- можливих шляхів проникнення порушника;
- режиму та тактики охорони;
- вимог маскуванню монтажу, дизайну.

Сповіщувач у процесі експлуатації піддається впливу різних перешкод та факторів, що заважають, серед яких основними є: акустичні перешкоди та шуми, вібрація будівельних конструкцій, рух повітря, електромагнітні перешкоди, зміни температури та вологості навколишнього середовища, перешкоди по мережі електроживлення. Ступінь впливу перешкод на роботу технічних засобів охоронної сигналізації залежить від їхньої потужності та принципу дії, а також схемно-технічних рішень апаратури.

Технічні засоби пожежної сигналізації.

Технічні засоби пожежної сигналізації умовно поділяють на групи за функціями, що виконуються: пожежні сповіщувачі, пожежні прилади приймально-контрольні та управління, пожежні оповіщувачі. Конструктивно технічні засоби пожежної сигналізації можуть бути виконані у вигляді блоків, що поєднують у собі функції декількох пристроїв, наприклад, приймально-контрольного приладу, приладу управління та джерела безперебійного живлення, або у вигляді окремих блоків, з'єднаних лініями зв'язку та розосереджених у просторі. Технічні вимоги до кожної з груп ТЗ та методи випробувань визначені відповідним нормативним документом.

Доцільність використання тих чи інших систем визначається вимогами конкретного об'єкта в залежності від завдань, що виконуються системою на об'єкті, його геометричних характеристик, необхідності можливостей переконфігурування та перепрограмування системи тощо.

Основною складовою систем автоматичного пожежогасіння є автоматичні пожежні сповіщувачі.

Вибір типу точкового димового пожежного сповіщувача рекомендується проводити відповідно до його здатності виявляти різні типи димів. Пожежні сповіщувачі полум'я слід застосовувати, якщо в зоні контролю у разі виникнення пожежі на його початковій стадії передбачається поява відкритого полум'я.

Спектральна чутливість сповіщувача полум'я повинна відповідати спектру випромінювання полум'я горючих матеріалів, що знаходяться у зоні контролю сповіщувача. Теплові пожежні сповіщувачі слід застосовувати, якщо у зоні контролю у разі виникнення пожежі на його початковій стадії передбачається значне тепловиділення.

Диференціальні та максимально диференціальні теплові пожежні сповіщувачі слід застосовувати для виявлення вогнища пожежі, якщо в зоні контролю не передбачається перепадів температури, не пов'язаних з виникненням пожежі, здатних викликати спрацювання пожежних сповіщувачів цих типів.

Газові пожежні сповіщувачі рекомендується застосовувати, якщо у зоні контролю у разі виникнення пожежі на його початковій стадії передбачається виділення певного виду газів у концентраціях, які можуть спричинити спрацювання сповіщувачів. Газові пожежні сповіщувачі не слід застосовувати в приміщеннях, в яких без пожежі можуть з'являтися гази в концентраціях, що викликають спрацювання сповіщувачів.

У тому випадку, коли в зоні контролю домінуючий фактор пожежі не визначений, рекомендується застосовувати комбінацію пожежних сповіщувачів, що реагують на різні фактори пожежі, або комбіновані пожежні сповіщувачі.

Пожежні сповіщувачі слід застосовувати відповідно до вимог державних стандартів, норм пожежної безпеки, технічної документації та з урахуванням кліматичних, механічних, електромагнітних та інших впливів у місцях їх розміщення.

Димові пожежні сповіщувачі, що живляться за шлейфом пожежної сигналізації та мають вбудований звуковий оповіщувач, рекомендується застосовувати для оперативного, локального оповіщення та визначення місця пожежі в приміщеннях, в яких одночасно виконуються такі умови [4, 11]:

- основним фактором виникнення вогнища загоряння у початковій стадії є поява диму;
- у приміщеннях, що захищаються, можлива присутність людей.

Такі сповіщувачі повинні включатися до єдиної системи пожежної сигналізації з виведенням тривожних сповіщень на прилад приймально-контрольний пожежний, розташований у приміщенні чергового персоналу.

Технічні засоби тривожної сигналізації.

Система тривожної сигналізації є сукупність спільно діючих технічних засобів, що дозволяють автоматично або вручну видавати сигнали тривоги на ПЦН (в чергову частину) при розбійному нападі на об'єкт у період його роботи.

Для оперативної передачі повідомлень до охоронних підприємств або ПЦН про напад злочинців об'єкт повинен бути обладнаний технічними засобами тривожної сигналізації (кнопки, педалі, оптико-електронні сповіщувачі тощо).

Такі пристрої встановлюють у сховищах цінностей, сейфових кімнатах, на службових місцях співробітників, які працюють із цінностями, у кабінетах керівника об'єкта, головного бухгалтера, кімнатах зберігання зброї та боєприпасів, біля дверей запасних виходів, на посту та у приміщенні охорони. Тривожними сповіщувачами рекомендується обладнати маршрути перенесення цінностей.

Систему тривожної сигналізації виконують з функцією "Без права відключення" та виводять через пульт внутрішньої охорони або безпосередньо на ПЦН, до чергової частини ОВС та пульт оперативного чергового охоронного підприємства.

Тривожною сигналізацією обов'язково оснащуються об'єкти підгрупи АІ, обмінні пункти, великі (головні) каси, ювелірні магазини, ломбарди, ювелірні майстерні.

Установи банків, поштові відділення, об'єкти із зберіганням наркотичних засобів та психотропних речовин, бланків суворої звітності відповідно до вимог нормативних документів узгоджених із МВС.

Необхідність оснащення тривожною сигналізацією інших об'єктів визначається комісією, яка приймає об'єкти під охорону.

Тривожна сигналізація може виконуватися як за допомогою дротових, так і бездротових сповіщувачів (радіокнопок, брелоків тощо). На об'єктах, на яких

ведуться операції з грошима, можуть встановлюватись автоматичні тривожні сповіщувачі (сповіщувач наявності останньої купюри тощо).

Тривожна сигналізація повинна забезпечувати зручність потайного (від злочинця) використання користувачем для виклику міліції або служби безпеки підприємства. При неможливості потайного використання ручних тривожних сповіщувачів (кнопок) необхідно використовувати ножні (педалі), бездротові тривожні сповіщувачі (радіокнопки, брелоки). При використанні тривожної сигналізації має бути забезпечена відсутність звукового сигналу у приміщенні, де вона була використана.

Склад системи охоронної сигналізації.

Залежно від масштабу завдань, які вирішує охоронна сигналізація, до її складу входить обладнання трьох основних категорій:

Обладнання централізованого управління охоронною сигналізацією (наприклад, центральний комп'ютер із встановленим на ньому ПЗ для управління охоронною сигналізацією; у невеликих системах охоронно-пожежної сигналізації завдання централізованого управління виконує охоронно-пожежна панель);

Обладнання збору та обробки інформації з датчиків охоронної сигналізації: прилади приймально-контрольні охоронно-пожежні (панелі);

Сенсорні пристрої - датчики та сповіщувачі охоронної сигналізації.

Інтеграція охоронної сигналізації у складі єдиної системи охоронно-пожежної сигналізації здійснюється на рівні централізованого моніторингу та управління. При цьому системи охоронної та пожежної сигналізації адмініструються незалежними один від одного постами управління, що зберігають автономність у складі системи охоронно-пожежної сигналізації.

На невеликих об'єктах охоронно-пожежна сигналізація керується приймально-контрольними приладами. Приймально-контрольний прилад здійснює живлення охоронних та пожежних сповіщувачів за шлейфами охоронно-пожежної сигналізації, прийом тривожних сповіщень від сповіщувачів, формує тривожні повідомлення, а також передає їх на станцію

централізованого спостереження та формує сигнали тривоги на спрацювання інших систем.

Особливості експлуатації різноманітних систем технічних засобів охорони.

Системи охоронної сигналізації відрізняються такими елементами:

По-перше, провідний зв'язок. Цей зв'язок передбачає підключення приймально-контрольного приладу з наявного телефонного зв'язку.

Плюсами даного зв'язку є те, що пульт централізованої охорони автоматично по даному зв'язку тестує на працездатність та спрацювання датчиків майже кожен хвилину. Однак, у разі спрацювання сигналізації датчика, підключеного у зв'язку з цим, господареві приміщення або обумовленій у договорі довіреній особі доведеться з'являтися до приміщення для перезапуску засобу охоронної сигналізації. Виклик здійснюється для відключення та ввімкнення живлення засобу охоронної сигналізації, з подальшим підтвердженням диспетчеру пульта централізованої охорони.

Другий вид – це GSM зв'язок. Для багатьох власників на сьогоднішній день цей вид підключення до пульта централізованої охорони є найпривабливішим. Втім, він має як позитивні, і негативні сторони. Суть цього зв'язку полягає в тому, що приймально-контрольний датчик виводиться на пристрій мобільного зв'язку, яким забезпечується власник об'єкта, що охороняється, від охоронної структури. Даний датчик схожий на засіб мобільного зв'язку, однак, відмінність в тому, що ця карта в даному приладі програмується на датчики системи охоронної сигналізації і пульт централізованої охорони. Після спроби проникнення датчики системи охоронної сигналізації миттєво передають звіт про місце та час проникнення на пульт централізованої охорони та власнику датчика засобу охоронної сигналізації, що призводить до того, що на спрацювання датчика зможуть виїхати і групи затримання охоронної структури, і сам власник. Даний прилад тестує на працездатність датчики і сам засіб охоронної сигналізації, за програмно заданим часом, тому вихід з ладу засобу охоронної сигналізації може призвести до

несвоєчасного реагування із затримкою в кілька хвилин. Тут є запасний та зручний варіант. При спрацюванні такого датчика зазвичай виїжджає група швидкого реагування охоронної структури і оглядає об'єкт. Якщо пошкодження не виявляються, то група чекає, поки датчик сам не відновиться, після чого повідомляє на пульт централізованої охорони, який у свою чергу повинен повідомити клієнта.

Третім видом, на якому здійснюють свою роботу системи охоронної сигналізації, є радіозв'язок. Даний вид зв'язку на сьогоднішній день все рідше застосовується з огляду на те, що спрацьовує при відключенні електроенергії, при займанні і йому потрібне постійне харчування. Запасних блоків живлення на цей випадок не передбачено. Проте, цей вид зв'язку як і надійно діє як та інші, причому найбільш економічний у матеріальному плані.

При спрацюванні сигналізації, групи оперативного реагування охоронної структури повинні прибути місце негайно протягом 2 -7 хвилин, втім, якщо інше не передбачено договорі. Тому його обов'язково необхідно ретельно вивчити і при складанні та підписанні відобразити всі необхідні моменти з урахуванням важливості та місцезнаходження об'єкта охорони. Зазвичай охоронна структура вказує у договорі прибуття місце групи оперативного реагування в найкоротші терміни. Таким чином, видно, що пульт централізованої охорони на сьогоднішній день є гарантом спокою громадян та організацій за своє майно, тому що невинно та цілодобово відстежує зміни системи охоронної сигналізації на об'єктах. Групи ж оперативного реагування працюють цілодобово і готові негайно відреагувати на спрацювання та припинити спробу проникнення на об'єкт. Зазвичай приватні охоронні підприємства, що обслуговують системи охоронної сигналізації, узгодять свою діяльність з органами МВС, які законними методами зможуть вам допомогти у відшкодуванні збитків, а також складуть для вас документальне підтвердження для надання страхової компанії, якщо ваше майно застраховане.

Статистика органів внутрішніх справ показує, що розкрадання майна з приміщень становлять основну частину вчинених злочинів. Для цього охоронні

підприємства встановлюють додаткові системи захисту, а саме поєднують кілька видів підключення до пульта централізованої охорони одночасно з відеоспостереженням для об'єктів з великою площею.

Класифікація систем керування технічними засобами охорони.

Для керування технічними засобами охорони використовуються:

- Системи охоронно-пожежної сигналізації;
- телевізійні системи відеоспостереження;
- системи тривожної сигналізації.

Системи управління охоронно-пожежною сигналізацією та тривожною сигналізацією розглянуті в інших розділах програми.

Телевізійні системи відеоспостереження та системи контролю та управління доступом не можуть використовуватися як додатковий рубіж охоронної сигналізації.

При оснащенні об'єктів системами охоронної сигналізації повинні передбачатися організаційні або технічні способи резервування системи у разі виходу з ладу окремих її елементів та передусім приймально-контрольних приладів.

Порядок вибору систем сигналізації для охорони об'єкту.

Вибір системи управління технічними засобами охорони залежить від варіанту охорони об'єкта, кількості приміщень, які підлягають охороні, характеру і структури розміщення цінностей.

Усі вразливі місця обладнуються охоронною сигналізацією. Проте, для деяких об'єктів такого захисту недостатньо. На особливо важливих об'єктах ряд приміщень оснащуються додатковими межами сигналізації, системами відеоспостереження.

На промислових підприємствах, базах, складах, установах банків та інших об'єктах необхідно створювати зовнішній рубіж відеоспостереження встановлюється за периметром огорожі (будівлі).

Системи контролю і управління доступу.

Традиційні системи контролю доступу ідентифікують користувача за допомогою ключа, введення картки або набору коду для дозволу доступу. Застосування контактних систем призводить до втрати часу під час маніпуляцій.

У багатьох областях, де не допустимі втрати часу на дії працівників, пов'язані зі звичайними системами, оптимальним рішенням є безконтактна система контролю доступу.

Система працює дистанційно у діапазоні низьких частот (50...150 кГц). Вона дозволяє здійснювати безконтактну ідентифікацію карток та запрограмованих у них кодових номерів. Дозволяє зчитувати код через такі матеріали, як одяг, сумки та стіни.

Незважаючи на проведення великої кількості перевірок, з метою безпеки цей процес відбувається для користувача автоматично і швидко. Для тих, хто має право доступу, входні двері здаються незачиненими.

Завдяки застосуванню безконтактної технології унеможливорюються маніпуляції зі зчитувачами. Дозвіл на ті чи інші дії дається виключно в підсистемах або центральному комп'ютері, які встановлюються на захищеному ділянці.

Навіть пошкодження зчитувача за жодних обставин не дасть можливості несанкціонованого відкриття дверей.

Зчитувачі насамперед на зовнішніх входах повинні монтуватися таким чином, щоб вони були закриті, або встановлюватися на захищених ділянках дверей або стін. Завдяки цьому зменшується також ризик пошкодження, а встановлені елементи стають недосяжними.

Кодування карток, з одного боку, збільшує безпеку щодо структурування номерів кодів і, з іншого боку, дозволяє гнучкіше формувати та розміщувати кодову інформацію.

Наявний у картці має обсяг інформації. Якщо картка втрачається, її одразу можна анулювати. Таким чином, виключається небезпека несанкціонованого доступу за допомогою втраченої або вкраденої картки.

Зчитувачі системи монтують у двері, рами дверей, перегородки/стіни та кабіни ліфта таким чином, щоб вони були повністю приховані від очей. В оформленні елементів, що зчитують, враховуються ергономічні та естетичні вимоги. Ядро системи знаходиться на захищеному ділянці.

Система має модульну побудову та окремі елементи можна легко замінити. Система може бути розширена без заміни наявної апаратури.

Можна поставити під контроль додаткові входи та під'їзди або ввести додаткові функції, наприклад, облік часу присутності співробітників або відвідувачів.

Контроль доступу перешкоджає:

- крадіжці, у тому числі особистих речей;
- промислового шпигунства;
- навмисне пошкодження майна;
- Створює бар'єр для "цікавих".

Контролюється заздалегідь заданий максимально дозволений час відкриття дверей. За надто тривалого часу відкриття подається сигнал тривоги. Перший сигнал тривоги дається акустично біля дверей. Це дозволяє закрити двері без будь-яких подальших наслідків. Якщо двері продовжують залишатися відчиненими, то дається основний сигнал тривоги з протоколюванням у головній системі.

Тривога може передаватися й у інше місце чи іншу систему.

За допомогою програмного забезпечення двері можуть відмикатися на певний період. Наприклад, двері можуть бути відчиненими, кожен робочий день з 8.00 до 17.00.

Можна також запрограмувати систему так, щоб відкриття вранці (з 8.00) здійснювалося лише після зчитування першої картки (наприклад, о 8.14, коли увійшла перша людина). Таким чином, відкриття дверей здійснюється лише тоді, коли у відповідній зоні знаходиться особа, яка має право на доступ.

Кожні двері за допомогою додаткових інтерфейсів можуть з'єднуватися з охоронною та протипожежною системою при подвійному контролі доступу.

Користування ліфтом може здійснюватися за допомогою картки. Певні поверхи можуть бути заблоковані, а вхід на них може здійснюватись лише за наявності права доступу. Можна також викликати ліфт на певні поверхи карткою замість кнопки виклику і цим обмежити користування ліфтом.

Відвідувачі можуть отримати право доступу у виділений для них час. Усі відвідування можуть фіксуватися з різними даними відвідувача.

Ця інформація зберігається в системі і може бути будь-якої миті запрошена за різними критеріями пошуку. Можна також роздрукувати для відвідувача перепустку з прізвищем, назвою фірми та датою.

Якщо при в'їзді водії автотранспорту триматимуть картку збоку біля вікна автомобіля, ідентифікація здійснюється автоматично на відстані. За наявності права доступу з центрального пульта передається сигнал відкриття воріт чи шлагбаума.

Передбачені спеціальні картки, які можуть кріпитися на автомобілях (наприклад, автомобілі директора, фірмових службових автомобілів тощо).

Картки, змонтовані на днищі автомобіля, автоматично зчитуються та перевіряються при перетині закладеної в полотно дороги петлі. Це дозволяє провести ідентифікацію без будь-яких операцій. Прихована дротяна петля захищена від будь-якого виду пошкоджень чи маніпуляцій.

Система контролю доступу дозволяє також реалізувати ковзний графік роботи працівників. При цьому картка може "наголошуватися" на терміналі обліку часу. Залежно від вимог та обсягу системи використовується один комп'ютер на дві області застосування або дві окремі системи.

Існує повне програмне забезпечення для обліку робочого часу співробітників. Структура цього рішення враховує вимоги, які найчастіше висуваються замовником, економить витрати і спрощує поводження з системою.

Системи комп'ютерного керування технічними засобами охорони.

Рівень безпеки об'єкта визначається ймовірністю його збереження від розкрадання чи знищення. Ступінь безпеки об'єкта залежить від своєчасного реагування технічних засобів охоронної та тривожної сигналізації на загрозу, що

виникає, і від часу подолання фізичних бар'єрів: решіток, замків, засувок на вікнах і дверях, спеціальним чином укріплених дверей, стін, підлог, стель та інших будівельних конструкцій, тобто засобів інженерно-технічного укріплення по дорозі можливого руху порушника. Чим раніше можна виявити загрозу об'єкту, тим швидше її можна припинити. Це досягається правильним вибором і застосуванням технічних засобів охоронної та тривожної сигналізації, їх правильним розміщенням в зонах, що охороняються.

Кошти інженерно-технічної укріпленості збільшують час, необхідний їх подолання, що створює можливість затримання порушника. Особливо це проявляється при поєднанні засобів інженерно-технічної укріпленості та технічних засобів охоронної та тривожної сигналізації. Засоби інженерно-технічної укріпленості, крім фізичної перешкоди, виконують функції психологічного бар'єру, що запобігає можливості проникнення порушника на об'єкт, що охороняється.

Об'єкт, що охороняється: підприємство, організація, житло, їх частина або комбінація, обладнані діючою системою охорони. Пульт централізованого спостереження: технічний засіб (сукупність технічних засобів) або складова частина системи передачі сповіщень, що встановлюється в пункті централізованої охорони, для прийому від пультових кінцевих пристроїв або ретрансляторів сповіщень про проникнення, розбійний напад на об'єкти, що охороняються, та (або) пожежі на них.

Пункт централізованої охорони: структурний підрозділ охоронного підприємства, що здійснює централізовану охорону об'єктів за допомогою пульта централізованого спостереження та забезпечує оперативний виїзд груп швидкого реагування, затримання на об'єкт, що охороняється, при надходженні з нього сповіщень про спрацювання сигналізації.

Рубіж охоронної сигналізації: шлейф або сукупність шлейфів сигналізації, що контролює зону території, будівлі або приміщення (периметр, обсяг або площу, цінності) на шляху можливого руху порушника до

матеріальних цінностей, при подоланні якої видається відповідне повідомлення про проникнення.

Шлейф сигналізації: електричний ланцюг, що з'єднує вихідні ланцюги охоронних сповіщувачів, що включають допоміжні (виносні) елементи (діоди, резистори тощо) і з'єднувальні дроти, і призначений для видачі на прилад приймально-контрольних повідомлень про проникнення (спроба проникнення) та несправності, а в деяких випадках – для подачі електроживлення на сповіщувачі.

Системи відеонагляду.

Системи відеоспостереження для дому дозволяють вирішити безліч питань, пов'язаних з оптимізацією новітньої системи безпеки. Системи відеоконтролю за об'єктом дають можливість створювати безперервний відеозапис, який в майбутньому зможе засвідчити справжність подій, що відбулися.

Відеоконтроль будинку відбувається за допомогою системи, що складається з камери відеоспостереження та монітора. Між ними проходить лінія зв'язку, якою інформація від камери надходить на монітор. Для великих розмірів об'єкта, що охороняється, в деяких зонах використовуються багатокамерні системи відеоспостереження, в яких зображення відображається на монітори через квадранти або мультиплексори. Найкращим є спостереження одним оператором із 4-х відеокамер.

Існує невелика кількість методів для здійснення системи відеоспостереження для дому:

На базі відеореєстратора.

Відеореєстратор - це цифровий пристрій, який призначений для спостереження та запису всього, що відбувається. Найчастіше реєстратор використовують як додатковий інструмент охоронних служб. Головним параметром кожного пристрою системи відеоспостереження - це кількість кадрів, що показуються на екрані, в одну секунду. Стандартом є величина, що становить 25 кадрів на секунду.

Багато відеореєстраторів можуть забезпечувати спостереження з такою частотою, але із записом відбувається трохи по-іншому. У документації зазвичай вказується загальна частота для всіх підключених камер. Наприклад, якщо пристрій записує відео з частотою 25 кадрів в секунду, дві включені камери поділять це число навпіл (тобто, по 12 кадрів в секунду). А якщо камер чотири, то частота буде близько 6 кадрів на секунду.

Одним з важливих параметрів реєстратора є максимальна роздільна здатність запису відео. Воно позначається двома цифрами: кількість пікселів, що відображаються, по горизонталі і по вертикалі. Чим більша роздільна здатність, тим чіткіше, якісніше і краще вийде зображення, тим самим будуть відображатися найдрібніші деталі на екрані монітора під час відтворення запису. Але варто пам'ятати, що на чіткість картинки також впливатиме точний вибір камер спостереження та об'єктивів.

Головна характеристика відеореєстратора - це самостійність та узгодженість функцій.

На основі відеосервера.

Відеосервер дозволяє розвивати мережеві системи відеоспостереження, не відмовляючись від аналогового обладнання. Відеосервер чудово підходить для інтеграції з аналоговими CCTV-системами. Даний пристрій додає нові функціональні можливості аналоговому устаткуванню та прибирає потребу у супутній периферії: у коаксильних кабелях, моніторах та відеореєстраторах. Відеореєстратори стають непотрібними, оскільки відеозапис може здійснюватися стандартними серверами на основі ПК.

Відеосервери зазвичай мають від одного до чотирьох аналогових портів для підключення камер та Ethernet-порт для підключення до мережі. Як і в мережеву камеру, відеосервер вбудовані веб-сервер, чіп, що здійснюють відеостиснення, і операційна система, тому вхідний аналоговий відеопотік може бути перетворений на цифровий, переданий або записаний через комп'ютерну мережу.

Бездротове відеоспостереження.

Дана система відеоспостереження - це найкраще рішення у зв'язку з відсутністю провідного способу. Головними приладами є бездротові камери.

Бездротові камери відеоспостереження оснащені функцією Wi-Fi, яка дозволяє їм підключатися до мережі бездротовим способом, що значно заощаджує кошти на підключення без витрат на кабель. Бездротові системи відеоспостереження можуть використовуватися як у приміщенні, так і на вулиці. Якщо Ви самостійно не зможете встановити та налаштувати бездротову відеокамеру, Ви завжди зможете звернутися до нас.

Система IP-відеоспостереження.



IP-камери відеоспостереження, по-іншому відомі як мережеві камери, будучи цифровими відеопристроями, є основним будівельним блоком для будь-якої сучасної системи відеоспостереження, в яких передача даних і управління системою здійснюється за допомогою протоколу комп'ютерної мережі IP (Internet Protocol).

Кожна IP-камера - це свого роду пристрій, що поєднує звичайну камеру спостереження з комп'ютером. Причому з можливістю безпосереднього підключення до IP-мереж.

IP-камери відеоспостереження, а також інші мережні пристрої мають свою власну IP-адресу, яка використовується для ідентифікації камери в мережах LAN/WAN/Internet. До складу систем відеоспостереження, побудованих на

основі IP-камер, як правило, входять веб-сервер, FTP-доступ, електронна пошта (e-mail), система управління аварійними сигналами. Більшість IP-камер мають додаткові рішення. Найпоширеніша додаткова опція - "розумний" аналіз зображення, який реально підвищує ефективність роботи IP-систем відеоспостереження. Інша опція, що часто зустрічається, — двосторонній аудіо-зв'язок, що дозволяє вести акустичний моніторинг приміщення, в якому працює IP-камера.

Системи відеоспостереження для дому бувають кольоровими чи чорно-білими. Чорно-білі системи набагато дешевші за кольорові і мають більшу роздільну здатність, але не передають деяку інформацію (колір волосся, одяг). Найважливіша характеристика відеосистеми — це дозвіл. Монітор повинен мати високу роздільну здатність, щоб не псувати дозвіл системи відеоконтролю.

Системи відеоспостереження для дому діляться на аналогові та цифрові. Для відеоспостереження на маленьких об'єктах та запису інформації на відеоманітофон найкраще застосовувати системи аналогового відеоспостереження. Цифрові системи забезпечують відеоспостереженням територіальні об'єкти, тому що підтримують режим перегляду в даний час, самотійний режим роботи, а також забезпечує хорошу якість запису та передачу запису на інші носії. Встановлення відеоспостереження вдома можна здійснювати з різними цілями:

- для додаткового забезпечення безпеки проживання;
- для організації контролю над членами сім'ї;
- підтримки дисципліни домашнього персоналу.

Здійснюючи встановлення відеоспостереження вдома, необхідно також враховувати низку нюансів. Насамперед слід взяти під візуальний контроль вхід на прибудинкову територію. Якщо є кілька входів у будинок, а також велика прибудинкова територія, то з метою безпеки необхідно брати під контроль місця, де найімовірнішим стає проникнення зловмисників. Як правило, додаткового спостереження потребують територія двору навколо будинку і гараж. З метою забезпечення конфіденційності відеоспостереження камери можуть маскуватися

або монтуватися в предмети ландшафтного дизайну. Якщо використовується обладнання відкритого типу, то доцільним стає використання додаткових кожухів та систем антивандального захисту.

2 АНАЛІЗ ІНЖЕНЕРНО-ПРОГРАМНОГО КОМПЛЕКСУ ТЕХНІЧНИХ ЗАСОБІВ СИСТЕМ БЕЗПЕКИ ОБ'ЄКТА

Інженерно-програмний комплекс технічних засобів Систем безпеки (далі – СБ) призначений для забезпечення безпеки співробітників і відвідувачів будівлі, та збереження матеріальних цінностей в приміщеннях і на прилеглій території шляхом комплексної охорони території об'єкту, виявлення на ранній стадії спроб проникнення в охороняємі зони, попередження служби безпеки.

До складу систем безпеки об'єкту входять:

- Система контролю доступу;
- Система охоронної сигналізації;
- Система відеоспостереження та відеоконтролю.

Система контролю доступу призначена для виявлення, застереження, обмеження входу/виходу відвідувачів та персоналу, а також запобігання несанкціонованого проникнення на територію зон обмеженого доступу, шляхом розмежування та безперервного контролю цих зон, реєстрації всіх подій в системі та видачі візуальної інформації про оперативний стан на об'єкті служби охорони.

Система охоронної сигналізації призначена для виявлення фактів несанкціонованого проникнення і злому приміщень об'єкту, що захищаються, за допомогою установки в них різних типів сповіщувачів.

Система відеоспостереження та відеоконтролю призначена для візуального виявлення небезпеки в зонах загального користування (вестибюль, ліфтові холи, коридори) на території, окремих технічних приміщеннях та по периметру будівлі шляхом отримання, передачі, реєстрації зображень зон спостереження від телекамер та видачі візуальної інформації про оперативну обстановку на об'єкті на автоматизовані робочі місця (далі - АРМ) служби безпеки.

2.1 Система контролю доступу

2.1.1. Основні проектні рішення СКД. Система контролю доступу є складовою комплексу систем безпеки об'єкту. Запроектована система контролю доступу має можливість взаємодії з іншими системами та можливість розширення у майбутньому.

Система контролю доступу спроектована на базі використання мережевих контролерів доступу, що забезпечують підключення:

- зчитувачів ідентифікаційної інформації;
- сповіщувачів стану положення дверей, що контролюються (відчинено/зачинено);
- виконавчих запираючих пристроїв.

У якості носія ідентифікаційної інформації використовуються пластикові картки доступу з форматом Mifare.

Для контролю за переміщенням людей на об'єкті використовуються безконтактні зчитувачі Proximity-карток. Для виходу з приміщень використовуються кнопки відчинення дверей.

Для блокування та розблокування відкриття дверей у підохоронних приміщеннях використовуються електромеханічні замки нормально відчиненого типу, що не вимагає додаткових засобів для розблокування дверей в разі зникнення електроживлення замка. Для доведення дверей до закритого положення використовуються довідники дверей механічні, які поставляються та встановлюються фірмою-виробником дверей.

Для одночасного розблокування усіх проходів, що контролюються СКД, у випадку надзвичайної ситуації (наприклад, під час стихійного лиха) в системі передбачається використання кнопки аварійного розблокування дверей. При отриманні системою контролю доступу сигналу "пожежа" від системи пожежної сигналізації усі проходи, що контролюються СКД, розблоковуються автоматично.

Для реєстрації, обробки, запису подій доступу крізь проходи, що контролюються в системі використовується сервер комплексу безпеки.

Для контролю за СКД, налаштування параметрів, а також для ініціалізації та видачі карток використовується автоматизоване робоче місце оператора, яке організовується на відмітці +3.300 1-ї черги об'єкта в приміщенні Операторської та складається з комп'ютеру зі спеціальним програмним забезпеченням, зчитувача карток та монітору, на який виводиться план об'єкту та протокол подій в системі.

2.1.2 Конфігурація системи СКД. Склад, розташування та характеристики складових системи визначені згідно до вимог завдання на проектування та можливості розширення комплексу в майбутньому. Конфігурацію СКД дивись арк. 3 «Система контролю доступу. Схема структурна».

Виконавчими пристроями системи контролю доступу обладнуються службові та адміністративні приміщення громадсько-торгівельного центру.

Керуючі мережеві контролери доступу розміщуються в комутаційних приміщеннях на відмітках -3.400, 0.000, +3.300 та +6.400. Всі контролери підключаються до локальної мережі Ethernet об'єкту, за допомогою мережевих комутаторів в комутаційних приміщеннях, для апаратної взаємодії всього обладнання СКД та для обміну даними з серверним обладнанням та автоматизованими робочими місцями операторів системи безпеки.

Обладнання електроживлення СКД розміщується в комутаційних приміщеннях на відмітках -3.400, 0.000, +3.300 та +6.400.

2.1.3 Функціонування системи СКД. Функціонування системи відбувається на основі технології proximity - дистанційного (безконтактного) зчитування ідентифікаційного ознаки. В якості ідентифікатора у системі контролю доступу всі співробітники використовують персональні proximity-карти із запрограмованим кодом формату Mifare. Після піднесення до зчитувача

proximity-карти, отриманий код передається на контролер. Контролер аналізує код, ідентифікує карту і приймає рішення про дозвіл або заборону проходу через контрольовану точку. Якщо власникові proximity-карти дозволений прохід в приміщення, після піднесення до зчитувача proximity-карти система подає сигнал на замок і розблокує двері. Для доведення дверей приміщень до закритого положення використовуються довідники дверей механічні. Вихід з приміщення здійснюється після натискання кнопки виходу. Система одержує інформацію про положення дверей (відчинені/зачинені) від сповіщувачів точкових магнітоконтактних.

2.2 Система охоронної сигналізації

2.2.1. Основні проектні рішення СОС. Система охоронної сигналізації є складовою комплексу систем безпеки об'єкту. Запроектована система має можливість взаємодії з іншими системами та можливість розширення у майбутньому.

Об'єкт оснащується багаторубіжною системою охоронної сигналізації з використанням сучасних технічних засобів.

Першим рубежем захищається периметр будівельних конструкцій. Зовнішні двері блокуються на відкриття магнітоконтактними сповіщувачами, вікна блокуються акустичними сповіщувачами розбиття скла. Другим рубежем СОС захищаються внутрішні об'єми приміщень сповіщувачами інфрачервоними пасивними руху та двері приміщень магнітоконтактними сповіщувачами.

Для виконання процедури постановки на охорону та зняття з під охорони приміщень об'єкту передбачається встановлення пультів керування на кожному поверсі.

В якості технічних засобів системи охоронної сигналізації проектом прийняті такі охоронно-тривожні сповіщувачі:

- пасивні інфрачервоні сповіщувачі руху – для блокування об'єму технічних, службових та адміністративних приміщень, об'єму торгівельних зон, службових сходових клітин;
- акустичні неадресні сповіщувачі розбиття скла;
- магнітоконтатні неадресні сповіщувачі;
- тривожні стаціонарні кнопки;
- радіокомплекти (приймачі, радіобрелки) для передачі сигналів тривоги з торгівельних зон служби охорони.

Для передачі співробітниками служби безпеки об'єкту сигналу тривоги на зовнішню охорону фірму - Управління Поліції охорони (УПО) передбачено тривожну кнопку на відмітці +3.300 1-ї черги об'єкта в приміщенні Операторської. Сигнал від тривожної кнопки за допомогою ППК фірми передається на пульт УПО по мережі GPRS.

Встановлення охоронно-тривожних сповіщувачів проводити згідно до вимог ВБН В.2.5-78.11.01-2003, особливостей приміщень, що захищаються та технічних характеристик сповіщувачів.

2.2.2. Конфігурація системи. Склад, розташування та характеристики складових системи визначені згідно до вимог завдання на проектування та можливості розширення комплексу в майбутньому. Конфігурацію СОС дивись арк. 4 «Система охоронної сигналізації. Схема структурна».

Керуюче обладнання СОС – Прилади прийомо-контрольні (далі – ППК) розміщуються в комутаційних приміщеннях на відмітках -3.400, 0.000, +3.300 та +6.400. Всі ППК підключаються за допомогою інтерфейсних кабельних з'єднань до керуючих мережевих контролерів доступу для обміну даними з серверним обладнанням та автоматизованими робочими місцями операторів системи безпеки.

Обладнання електроживлення СОС розміщується в комутаційних приміщеннях на відмітках -3.400, 0.000, +3.300 та +6.400.

2.2.3. Функціонування системи. Відкриття дверей, розбиття скла, попадання людини в зону дії сповіщувача, натиснення тривожної кнопки призводить до спрацювання відповідної зони системи охоронної сигналізації. Система також отримує сигнал "тривога" при повному знеструмленні обладнання та спробі взлому корпусів обладнання. Для запобігання взлому корпусів сповіщувачів та обладнання призначені їх тамперні зони, які постійно контролюються системою охоронної сигналізації та ніколи не знімаються з під охорони. Усі тривожні події фіксує ППК, до якого підключений сповіщувач, що спрацював. Тривожна інформація від ППК через локальну мережу надходить до серверу комплексу безпеки, що реєструє усі події в системі із зазначенням дати та часу подій в протоколі та зберігає їх на жорсткому диску впродовж 30 діб. Через локальну мережу безпеки усі події від серверу комплексу безпеки надходять на автоматизовані робочі місця.

2.3 Система відеоспостереження та відеоконтролю

2.3.1. Основні проектні рішення СВН. Для отримання відеозображень від телекамер, реєстрації, цифрової обробки і зберігання відеоінформації в СВН використовуються відеосервери, що забезпечують створення 30-денного відеоархіву по кожній телекамері в системі за умови середнього часу запису по детектору руху 12 годин на добу.

Призначенням телекамер, встановлених на об'єкті, є передача відеозображень про оперативну обстановку і про переміщення людей і товарно-матеріальних цінностей у приміщеннях об'єкта та на прилеглий території. Призначенням зовнішніх телекамер, що встановлюються на фасаді об'єкту є передача відеоінформації про обстановку на визначених зовнішніх підохоронних зонах фасаду, в'їзду/виїзду з паркінгу. Призначенням зовнішніх телекамер, що встановлюються в паркінгу об'єкту є передача відеоінформації про обстановку на території паркінгу. Усі зовнішні телекамери захищаються термокожухами, а

також пристроями грозозахисту (крім телекамер паркінгу). Для відеоконтролю за внутрішніми зонами об'єкту використовуються кольорові купольні телекамери та роботизовані телекамери.

Конкретні місця розташування телекамер визначаються з урахуванням необхідності забезпечення максимальної зони огляду і достатньої величини зображення об'єктів спостереження в найбільш відповідальних точках охоронних зон.

2.3.2 Конфігурація системи СВН. Склад, розташування та характеристики складових системи визначені згідно до вимог технічного завдання та можливості розширення комплексу в майбутньому. Конфігурацію СВН дивись арк. 5 «Система відеоспостереження та відеоконтролю. Схема структурна».

Обладнання обробки сигналів та електроживлення СВН розміщується в комутаційних приміщеннях на відмітках -3.400, 0.000, +3.300 та +6.400.

Живлення відеокамер забезпечують мережеві комутатори використовуючи технологію Power over Ethernet (PoE).

Для забезпечення відеоспостереження усередині приміщення проектом прийняті купольні кольорові мережеві відеокамери, що дозволяють забезпечити відео контроль за наступними зонами об'єкту:

- вестибюлі, коридори, тамбури, ліфтові холи, сходові клітини;
- торгівельні зони магазинів, установ громадського харчування та зон відпочинку;
- службові, адміністративні та технологічні приміщення.

Для забезпечення відеоспостереження на прилеглій території будівлі, та в зоні паркінгу проектом прийняті відеокамери кольорові вуличні із ІЧ підсвічуванням.

Запроектована СВН має можливість розширення в майбутньому.

2.3.3 Функціонування системи СВН. Встановлені телекамери формують цифровий відеосигнал з зображенням підохоронних зон і передають їх на відео сервери. Сервери приймають і оброблюють інформацію, записуючи її на жорсткі диски у вигляді відеоархіву.

Для онлайн моніторингу система відеонагляду передбачає клієнт-серверну побудову взаємодії керуючого обладнання. По локальній мережі за допомогою віддаленого підключення до керуючого відеосерверу через Web-інтерфейс виводиться відеоінформація на монітори АРМ, де здійснюється її перегляд, дистанційний контроль і управління СВН.

Для передачі відеосигналу від відеокамер до відеосерверів і для передачі живлення відеокамер використовується ІР-мережа.

СВН функціонує під управлінням спеціалізованого програмного забезпечення.

Програмне забезпечення встановлюється на відео серверах та автоматизованих робочих місцях і забезпечує на програмному рівні управління СВН.

Програмне забезпечення СВН функціонує на базі ліцензійної операційної системи і має спеціальний інтерфейс, який дозволяє зручно і наочно працювати з інформацією в СВН.

Програмне забезпечення СВН дозволяє забезпечити:

- виведення відео-зображень і аудіо-сигналів на робочі місця з можливістю локального й віддаленого запису у відеоархів;
- програмно реалізований механізм оптимізації потоків відеоінформації в розподіленій цифровій системі відеоспостереження при обмеженій пропускній здатності каналів зв'язки;
- одночасне виведення на Монітор відеоспостереження зображень, що надходять від декількох відеокамер (які підключені до одного або декількох відеосерверів) на одному екрані (дисплеї) комп'ютера;

- пріоритетне виведення відеозображень від тривожних або активних відеокамер;
- зміну кількості вікон відеоспостереження і їх розкладки на моніторі;
- виведення збільшеного відеозображення, що надходить від вибраної відеокамери;
- колірну індикацію стану вікна відеоспостереження (відеокамери) з відображенням станів: “На охороні”, “Тривожна”, “Запис” та ін.;
- можливість та вбудовані функції управління поворотними пристроями камер відеоспостереження;
- запис відеозображень з використанням алгоритмів стискування відеозображення (в залежності від джерела походження відеосигналу) Motion Wavelet (усіх версій), Wavelet 2000, Motion JPEG, MPEG-4, H.264 у наступних режимах: режим тривалого (постійного) відеозапису; режим запису в реальному часі по заданих подіях; запис по тривозі або по запиту оператора з передісторією.
- підтримка корпоративних стандартів ONVIF, ONVIF v.2.x, RTSP і PSIA;
- відображення стоп-кадру по команді оператора без зупинки запису;
- створення в автоматичному режимі або за розкладом резервних копій відеозаписів на виділеному сервері архіву, з можливістю проріджування відеокадрів;
- виведення на монітор відеоспостереження службової інформації: поточного часу; поточної дати; номера, найменування відеокамери.
- відеоспостереження й перегляд архіву з використанням Web-Інтерфейсу (ноутбук, КПК, мобільний телефон);
- ведення локального й мережного аудіо- й відео-архіву;
- перегляд відеозаписів з можливістю пошуку в архівах за часом, подією, відеокамерою;
- одночасне й синхронне відтворення відеозаписів по декількох відеокамерах;

- хронометрування архівних відеозаписів;
- пошук записів по тимчасових оцінках;
- обробка відео-зображення: цифрове збільшення; контрастування; фокусування; маскування; динамічне оконтурювання.
- керування поворотними пристроями з використанням таких засобів на підставі пріоритету: програмної інтерфейсної панелі стороннього виробника; універсальної панелі керування виконавчими пристроями; маніпулятора “миша”; маніпулятора “джойстик”;
- перегляд відеоінформації, що надходить із усіх наявних у системі відеосерверів, на робочих місцях з використанням комунікаційного середовища TCP/IP;
- збереження й експорт відеокадрів і відеозаписів у стандартні формати –AVI, MPEG, Divx і інші;
- збереження й експорт кадру відео-архіву в графічні формати BMP та JPG;
- друкування кадру архіву на принтер;
- можливість активації вбудованих модулів аудіо-аналітики (детектування пострілу, спрацювання авто-сигналізації);
- комплексне використання багато зонних детекторів таких типів: Руху; Фокусування; Стабільності відеосигналу; Зміни фону відео-зображення; Засвічення об’єктива відеокамери; Закриття об’єктива відеокамери; Залишених предметів; Інфрачервоний; детектор лиць осіб;
- детектор “трекер” об’єктів. Зона детектування: лінія або багатокутник:
 - детектор налаштовується на взаємодію з будь-яким об’єктом;
 - детектор налаштовується на взаємодію з людиною;
 - детектор налаштовується на взаємодію з автомобілем;
 - детектор спрацьовує при вході об’єкта в зону;
 - детектор спрацьовує при виході об’єкта із зони;

- детектор спрацьовує з появою об'єкта в зоні;
- детектор спрацьовує при зникненні об'єкта в зоні;
- детектор спрацьовує при зупинці об'єкта в зоні;
- детектор спрацьовує при знаходженні об'єкта в зоні більш 10 сек;
- детектор спрацьовує при залишеному предметі в зоні;
- аналітичний пошук по архіву із завданням умов пошуку за контентом й ознаками (область, напрямок руху, швидкість, колір);
- детектор “трекер” об'єктів при пошуку в архіві. Зона детектування: лінія, ламана лінія або багатокутник:
 - будуть знайдені відеозаписи будь-якого руху в області;
 - будуть знайдені відеозаписи, у яких здійснюється вхід об'єкта в область;
 - будуть знайдені відеозаписи, у яких здійснюється вихід об'єкта з області;
 - будуть знайдені відеозаписи, у яких відбувається поява об'єкта в області;
 - будуть знайдені відеозаписи, у яких відбувається зникнення об'єкта в області;
 - будуть знайдені відеозаписи, у яких об'єкт зупиняється в області;
 - будуть знайдені відеозаписи, на яких об'єкт перебуває в області більше 10 секунд;
 - будуть знайдені відеозаписи, на яких в області є залишений предмет;
 - використання маски зони детектора;
 - використання деінтерлейсинга.

Програмне забезпечення СВН для аналітичних функцій роботи системи забезпечує на об'єкті наступні можливості:

- можливість активації вбудованого програмно-аналітичного модуля торгової аналітики підрахунку людей (об'єктів) в зоні;

- можливість активації вбудованого програмно-аналітичного модуля торгової аналітики підрахунку відвідувачів;
- можливість активації вбудованого програмно-аналітичного модуля торгової аналітики гарячих-холодних зон;
- можливість активації вбудованого програмно-аналітичного модуля торгової аналітики гендерної та вікової приналежності;
- можливість активації вбудованого програмно-аналітичного модуля торгової аналітики підрахунку унікальних відвідувачів на базі розпізнавання обличь;
- можливість активації для кожного вбудованого модуля торгової аналітики та трекінгу функцій підвищення точності результатів за рахунок нейро-мереж, нейро-трекерів та нейро-фільтрів.
- можливість активації вбудованого програмно-аналітичного модуля пошуку обличь в архіві;
- можливість активації вбудованого програмно-аналітичного модуля розпізнавання обличь онлайн (білий/чорний список).

Устаткування системи відеоспостереження (робочі станції, мережеві відео сервери) підключити до мережі гарантованого електроживлення, що забезпечується джерелом безперебійного живлення.

Система цифрового запису забезпечує безперервну запис протягом 24 годин, а також забезпечує одночасний перегляд живого відео, архівації відеоінформації і перегляд архіву.

Конфігурація відеосерверів дозволяє записувати телекамери зі швидкістю до 25 кадрів в секунду. Запис відеоінформації на жорсткі диски відбувається тільки при наявності руху в полі зору телекамер, або по команді оператора.

Система забезпечує можливість організації окремих робочих місць як з повними можливостями з управління системою відеоспостереження, так і з обмеженими можливостями відповідно до рівня повноважень користувача.

Відеосервери забезпечують триплексний режим роботи (перегляд в режимі реального часу, запис, а також перегляд і копіювання записаної інформації в один і той же час), відеосервер дозволяє:

- переглядати відеозображення в режимі реального часу;
- вести безперервну запис зображення від всіх відеокамер;
- здійснювати пошук відеоінформації за різними критеріями (дата, час, подія);
- переглядати журнал подій;
- експортувати відеозображення;
- захищати систему і інформацію від несанкціонованого доступу паролями.

Функція "попереднього запису" дозволяє виконувати автоматичний запис подій зазначеної тривалості, що відбувалися до моменту виявлення руху в полі зору телекамер.

Таким чином, був проведений аналіз інженерно-програмного комплексу технічних засобів СБ об'єкту. Технічні засоби СБ складаються із системи охоронної сигналізації, системи контролю доступу та системи відеоспостереження та відеоконтролю. Кожна з цих систем виконує свої обов'язки, але тільки об'єднання цих систем в єдину інтегровану надає можливість організувати ефективну охорону сучасних особливих об'єктів.

3. ДОСЛІДЖЕННЯ ІНТЕГРОВАНОГО АПАРАТНО-ПРОГРАМНОГО КОМПЛЕКСУ БЕЗПЕКИ ОБ'ЄКТУ

Системи, що впроваджуються на об'єкті реалізовані в площині єдиного комплексу забезпечення безпеки на базі інтегрованого апаратно-програмного комплексу (далі – ІКБ), що забезпечує взаємодію систем контролю доступу, охоронної сигналізації, відеоспостереження та відеоконтролю між собою на протокольному рівні, та повністю сумісні з системами безпеки, що встановлені на об'єкті в частині 1-ї та 2-ї черги будівництва.

Всі підсистеми, що входять до складу ІКБ об'єднані за допомогою програмної, мережевої та апаратної взаємодії, що забезпечує можливість використання гнучкої логіки адміністрування ІКБ відповідно до заданих замовником алгоритмів охорони об'єкту.

Функціонування апаратно-програмного комплексу ІКБ відбувається з врахуванням всіх систем, які входять до складу комплексу. Алгоритми функціонування систем враховують події, які відбуваються в інших системах ІКБ.

3.1 Дослідження можливостей роботи програмно-апаратного комплексу побудови ІКБ

Програмно-апаратний комплекс побудови ІКБ забезпечує на об'єкті наступні можливості роботи:

- одержання й обробку даних від усіх підключених до нього підсистем, а також будь-яких пристроїв, включаючи перегляд відеопотоків із встановлених камер у реальному часі, роботу з відеоархівом, журналом подій і таке інше;
- оперативне реагування на тривоги будь-якого походження й контролювання технічного стану компонентів як власних підсистем, так і підсистем нижнього рівня;
- конфігурування розподіленої системи безпеки;

- збирання та обробку інформації від елементів всіх систем безпеки, що входять до його складу – СКД, СОС та СВН;
- фіксацію (архівування) отриманої інформації та результатів обробки на строк не менше 14 діб з функцією перезапису “по кільцю” (затирання даних, які мають дату створення більше ніж 14 діб назад);
- контроль і протоколювання дій операторів як моніторингових центрів так і локальних підсистем;
- функціонування всіх баз даних, що відносяться до ІКБ.

3.2 Дослідження можливостей і характеристик платформи ІКБ та програмного забезпечення

Платформа ІКБ та програмне забезпечення, що її реалізує має наступні можливості та характеристики:

- платформа ІКБ являється модульною;
- підтримується розподілені обчислення різними модулями відеоаналітики для одного і того ж відеопотоку;
- програмний комплекс ІКБ вбудований RTSP та WEB сервери, а також вбудований інтерпретатор скриптів (Microsoft jScript);
- у платформі ІКБ передбачена можливість активації вбудованої системи керування базами даних (далі – СКБД) графічної метайнформації для функцій інтелектуального пошуку в архіві (VMDA);
- система має окремий модуль-пакет драйверів (встановлення та видалення не впливає на роботу системи) для підключення (інтеграції) IP відео камер різних моделей (за API виробників камер);
- програмний комплекс ІКБ має безкоштовні оновлення;
- платформа ІКБ являється відкритою для зовнішньої інтеграції з використанням SDK як за допомогою підключаємих бібліотек, так і за

допомогою HTTP запитів (HTTP API), що дозволяє повністю управляти всіма елементами підсистеми, одержувати події й відсилати команди (реакції);

- система має можливість централізованої реєстрації й обробки подій, що надходять від підсистем, генерацію сповіщень (повідомлень) і керуючих впливів відповідно до алгоритмів, що гнучко настроюються;
- платформа ІКБ має легку масштабованість, відсутність програмних обмежень (окрім ліцензійних) на кількість будь-яких об'єктів у системі, а також має програмно необмежені можливості масштабування, адаптації до специфіки розв'язуваних завдань, перерозподілу використовуваних ресурсів при зміні кількості або якості завдань з моніторингу стану підконтрольних об'єктів і керування різного роду устаткуванням;
- система має можливість кластеризації компонентів підсистем, що дозволяє, при виході з ладу основного компонента підсистеми, продовжити виконання покладених на нього функцій, підключивши резервний компонент;
- платформа ІКБ має віддалену взаємодію центральних компонентів підсистем й автоматичну реплікацію внутрішніх баз даних (які містять параметри настроювання/налаштування системи й дані про зареєстровані у системі події), що входять до складу інтегрованого комплексу безпеки;
- система має програмний і апаратний контроль працездатності центральних компонентів системи;
- платформа ІКБ має можливість формування звітів по подіях на базі WEB та підтримує можливість автоматичного оповіщення (повідомлення) про події із застосуванням таких засобів: SMS (short message service); електронних поштових повідомлень; сервісу “v-dial” – автоматичного додзвону; звукового (голосового) оповіщення;
- програмний комплекс ІКБ має централізоване адміністрування компонентів системи, прав і повноважень користувачів.

3.3 Дослідження можливостей програмного забезпечення для відеоспостереження та сервісної відео аналітики

Програмне забезпечення програмно-апаратного комплексу побудови ІКБ для відеоспостереження та сервісної відеоаналітики має змогу налаштувань із урахуванням наступних вимог:

- виведення відеозображень на робочі місця з можливістю локального й віддаленого запису у відеоархів;
- програмно реалізований механізм оптимізації потоків відеоінформації в розподіленій цифровій системі відеоспостереження при обмеженій пропускній здатності каналів зв'язки;
- одночасне виведення на Монітор відеоспостереження зображень, що надходять від декількох відеокамер (які підключені до одного або декількох відеосерверів) на одному екрані (дисплеї) комп'ютера;
- зміна кількості вікон відеоспостереження і їх розкладки на моніторі;
- виведення збільшеного відеозображення, що надходить від вибраної відеокамери;
- колірна індикація стану вікна відеоспостереження (відеокамери) з відображенням станів: "На охороні", "Тривожна", "Запис" і т.і.;
- запис відеозображень з використанням алгоритмів стискування відеозображення H.264 у наступних режимах: режим тривалого (постійного) відеозапису; режим запису в реальному часі по заданих подіях; запис по тривозі або по запиту оператора з передісторією (передзаписом).
- використання при необхідності корпоративних стандартів ONVIF, ONVIF v.2.x, RTSP;
- відображення стоп-кадру по команді оператора без зупинки запису;
- виведення на монітор відеоспостереження службової інформації: поточного часу; поточної дати, номера, найменування відеокамери;

- відеоспостереження й перегляд архіву з використанням Web-інтерфейсу (ноутбук, КПК, мобільний телефон);
- перегляд відеозаписів з можливістю пошуку в архівах за часом, подією, відеокамерою;
- одночасне й синхронне відтворення відеозаписів по декількох відеокамерах;
- обробка відеозображення: цифрове збільшення; контрастування; фокусування; маскування; динамічне оконтурювання;
- збереження й експорт відеокадрів і відеозаписів у стандартні формати - AVI, MPEG, Divx і інші;
- збереження й експорт кадру відеоархіву в графічні формати BMP та JPG;
- друкування кадру архіву на принтер;
- комплексне використання багатозонних детекторів таких типів: Руху; Фокусування; Стабільності відеосигналу; Зміни фону відеозображення; Засвічення об'єктива відеокамери; Закриття об'єктива відеокамери; Залишених предметів; інфрачервоний; детектор лиць осіб.

ПЗ комплексу безпеки дозволяє організувати розмежування прав доступу:

- функціональні ролі:
 - "Адміністратор ";
 - "Оператор моніторингового центру ";
- внутрішні користувачі, тобто адміністративний й експлуатаційний персонал системи отримують доступ також з урахуванням наданих адміністратором системи прав та рівнів доступу;

Повний перелік функцій що мають бути налаштовані, відкоригувати на етапах дослідної експлуатації та приймання/здавання до постійної експлуатації.

3.4 Дослідження лінгвістичного забезпечення

Лінгвістичне забезпечення з забезпечує використання:

- української мови при розробці інтерфейсу користувача системи та вихідних документів (відеограм, машинограм тощо) і повідомлень Системи;
- української мови при формуванні та наповненні інформаційної бази системи;
- української мови при розробці й оформленні проектної та експлуатаційної документації системи;
- документація до купленого програмного забезпечення (у паперовому та/або електронному вигляді) може бути викладена англійською, російською або українською мовою відповідно до умов виробництва такого програмного забезпечення та комплекту постачання.

Захист від несанкціонованого доступу здійснюється шляхом санкціонування та обмеження доступу до:

- операційних систем серверів та АРМ;
- відеокамер;
- програмного забезпечення обчислювальних мереж та підпорядкованих підприємств (організацій, установ), які здійснюють обмін, приймання та передачу даних;
- прикладного програмного забезпечення системи;
- інформаційного забезпечення системи, включаючи бази даних;
- а також з шляхом створення та запровадження системи паролів (первинної генерації, збереження, розповсюдження, обліку, заміни, блокування та в цілому, системи, її супроводу як в частині створення, обліку, збереження тощо окремих паролів так і парольних книжок і т.і.).

3.5 Дослідження механізму автоматизованого контролю, аналізу інформації моніторингу, прогнозування ситуацій з масовим перебуванням людей

Передбачено механізми автоматизованого контролю, аналізу інформації моніторингу, прогнозування ситуацій, інваріантної реакції на ситуації стосовно до завдань адміністрації об'єкту з масовим перебуванням людей.

Додатково передбачено:

- резервування програмних засобів, що забезпечують інформаційний обмін між АРМ та серверним комплексом системи;
- виключення можливості випадкового руйнування програмного та інформаційного забезпечення внаслідок некоректних або навмисних дій користувача, шляхом розроблення спеціальних програмних засобів захисту та запровадження інших організаційно технічних заходів;
- можливість імпортування необхідних довідкових та інших даних із зовнішніх джерел (АС, систем, підсистем тощо, сторонніх підприємств, установ, організацій) та/або можливість послідовного ручного вводу поодиноких записів окремих довідників (класифікаторів) у базу даних нормативно-довідкової інформації або поодиноких записів іншого призначення;
- можливість взаємодії з іншими автоматизованими системами (підсистемами) як шляхом обміну експортованими (імпортованими) даними (файлами) з використанням засобів файлової системи операційної системи та/або засобами електронної пошти, так і в подальшому шляхом організації безпосереднього зв'язку відповідних баз даних.

Передбачено подальший розвиток та модернізація за рахунок можливостей:

- екстенсивного розвитку комплексів задач моніторингу за рахунок збільшення кількості місць встановлення відеокамер;
- розширення цільової користувацької аудиторії (збільшення числа користувачів та залучення додаткових груп користувачів за рахунок розвитку

інфраструктури Системи та послідовного нарощування номенклатури інформаційних послуг);

- розширення складу інформації контенту;
- модернізація технічних і програмних засобів (у частині кількісного та якісного розширення номенклатури відеообладнання, що підключається до Системи, наприклад, підключення додаткових сучасних відеокамер, а також у частині розширення функціональності без виведення з постійної експлуатації й без втрати даних Системи;
- вдосконалення Системи за рахунок постійного нарощування функціональних можливостей підсистеми аудіо- та відеоконтролю й відеоаналитики;
- розроблення конструкторів документів та пошукових запитів з розвиненою метамовою;
- розроблення засобів автоматичної інтеграції комплексів задач формування регламентних відповідей (звітів) та інших електронних документів, які збираються.

3.6 Дослідження параметрів системи відеоспостереження та відеоконтролю

3.6.1 Дослідження кута поля зору відеокамер. Для задач виявлення, як правило, краще мати поле зору, отримане з більш високої точки спостереження. Це допомагає уникнути перешкод, дозволяє краще зрозуміти поточний напрямок руху об'єкта і його потенційну траєкторію [9, 12]. Однак поле зору з високою точки не завжди сприяє завданням ідентифікації особи або одягу, тому що в цьому випадку обличчя або одяг видно під кутом або можуть бути закриті головним убором. Справедливо і зворотне: поле зору з більш низької точки дає кращі результати ідентифікації, але потенційно гірше дозволяє вирішувати завдання стеження і виявлення. Ще раз, помилка полягає не в тому, яке у

вашої камери поле зору, високе або низьке, а в нерозумінні переваг і недоліків кожного варіанту. Також помилкою буде не використовувати інформацію про призначення камери при виборі оптимальної висоти під час налаштування поля зору камери.

Для організації системи відеоспостереження необхідно розрахувати кількість відеокамер, що визначається із умови забезпечення не пропуску порушника із необхідною ймовірністю. Кожна камера характеризується певним кутом поля зору.

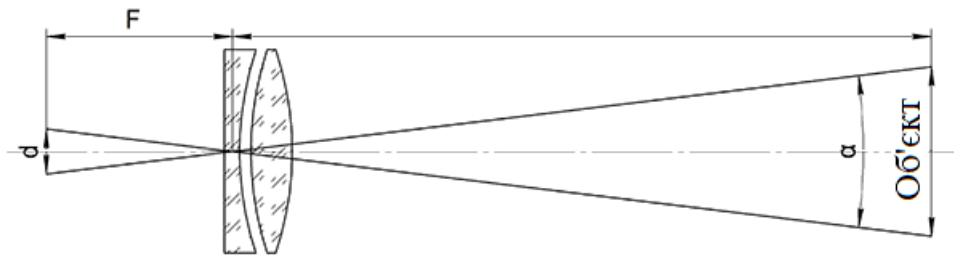


Рисунок 3.1 – Кут поля зору відеокамери

При виборі фокусної відстані об'єктива слід враховувати, що кут ясного зору людини по горизонталі становить приблизно 36° , що відповідає фокусній відстані $\sim 6,9$ мм (для відеокамери розміром матриці 1/3"). Тому відеокамери з фокусною відстанню об'єктива менше 6,9 мм візуально віддалятимуть зображення, більше 6,9 мм – відповідно наближатимуть.

Кут поля зору відеокамери розраховується за формулою:

$$\alpha = 2 \arctg \left(\frac{d}{2f} \right), \quad (3.1)$$

де d – розмір матриці, f – фокусна відстань.

Проведемо дослідження залежності кута поля зору від зміни фокусної відстані.

Відеокамера №1. Внутрішня купольна мережева відеокамера з параметрами не гірше: 5MP, кодек H.265, об'єктив - 2.7-13.5mm, інфрачервоне підсвічування - до 50 м ,

WDR.

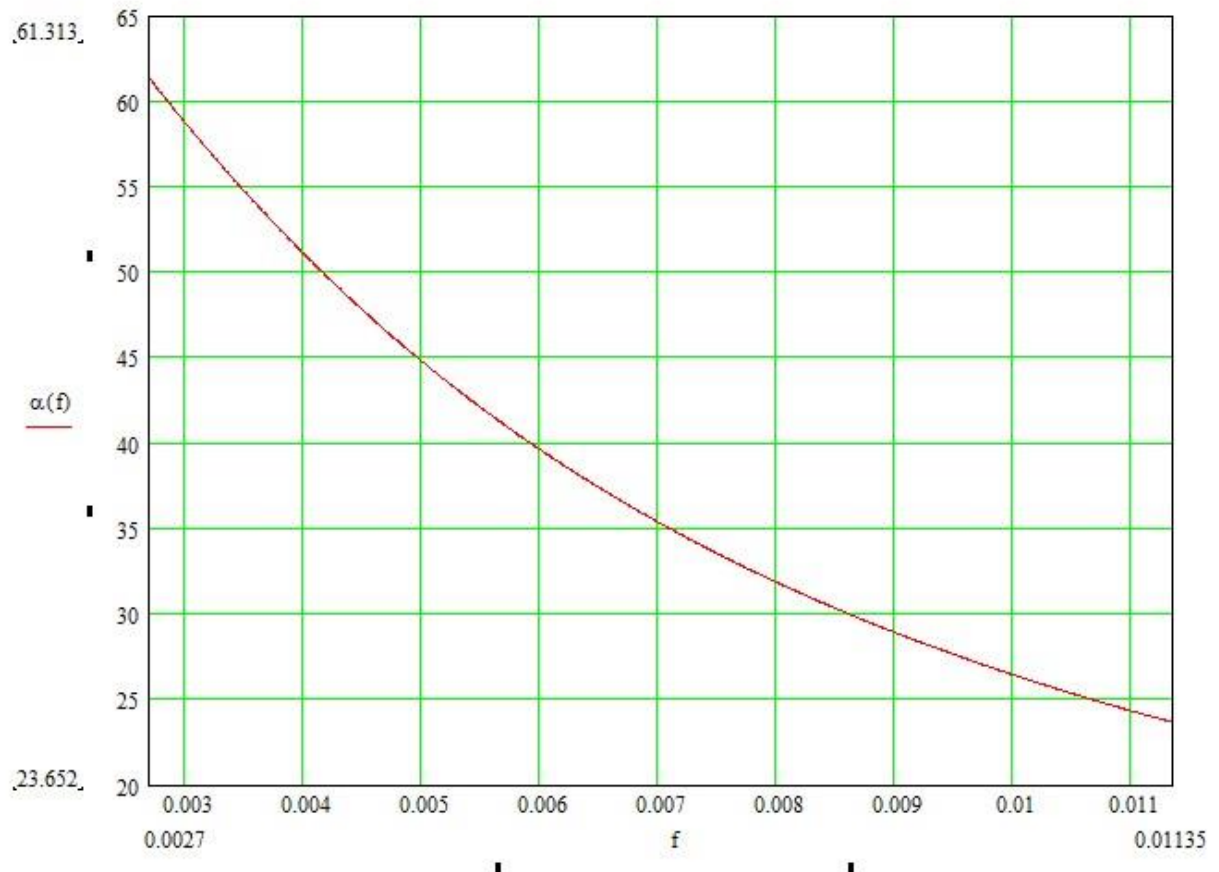


Рисунок 3.2 – Залежність кута поля зору відеокамери №1 від фокусної відстані

Відеокамера №2. Зовнішня циліндрична мережева відеокамера з параметрами не гірше: 5MP, кодек H.265, об'єктив - 4-9mm, інфрачервоне підсвічування - до 30 м , WDR.

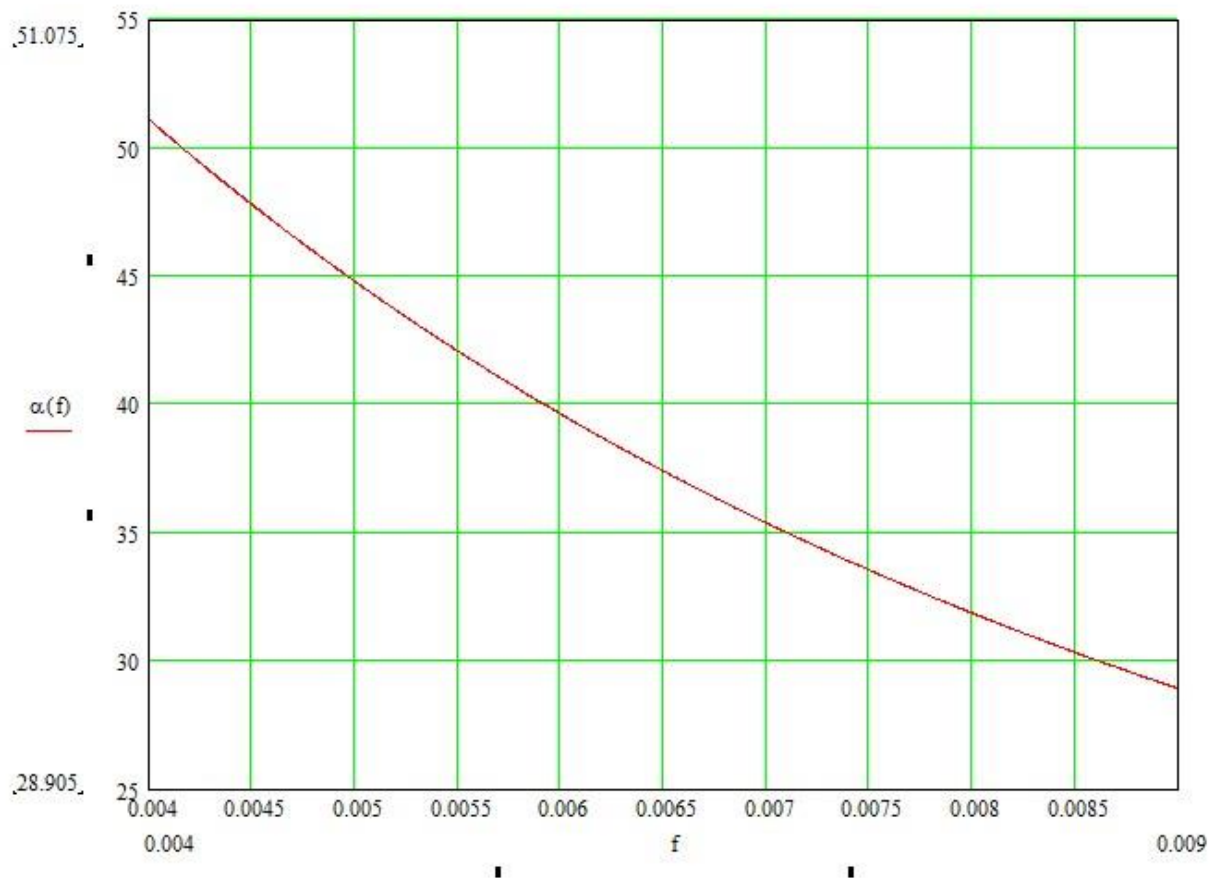


Рисунок 3.3 – Залежність кута поля зору відеокамери №2 від фокусної відстані

Відеокамера №3. Внутрішня мультисенсорна мережева відеокамера з параметрами не гірше: 20MP, 4 моторизовані об'єктиви - 3.7-7.7мм, WDR pro.

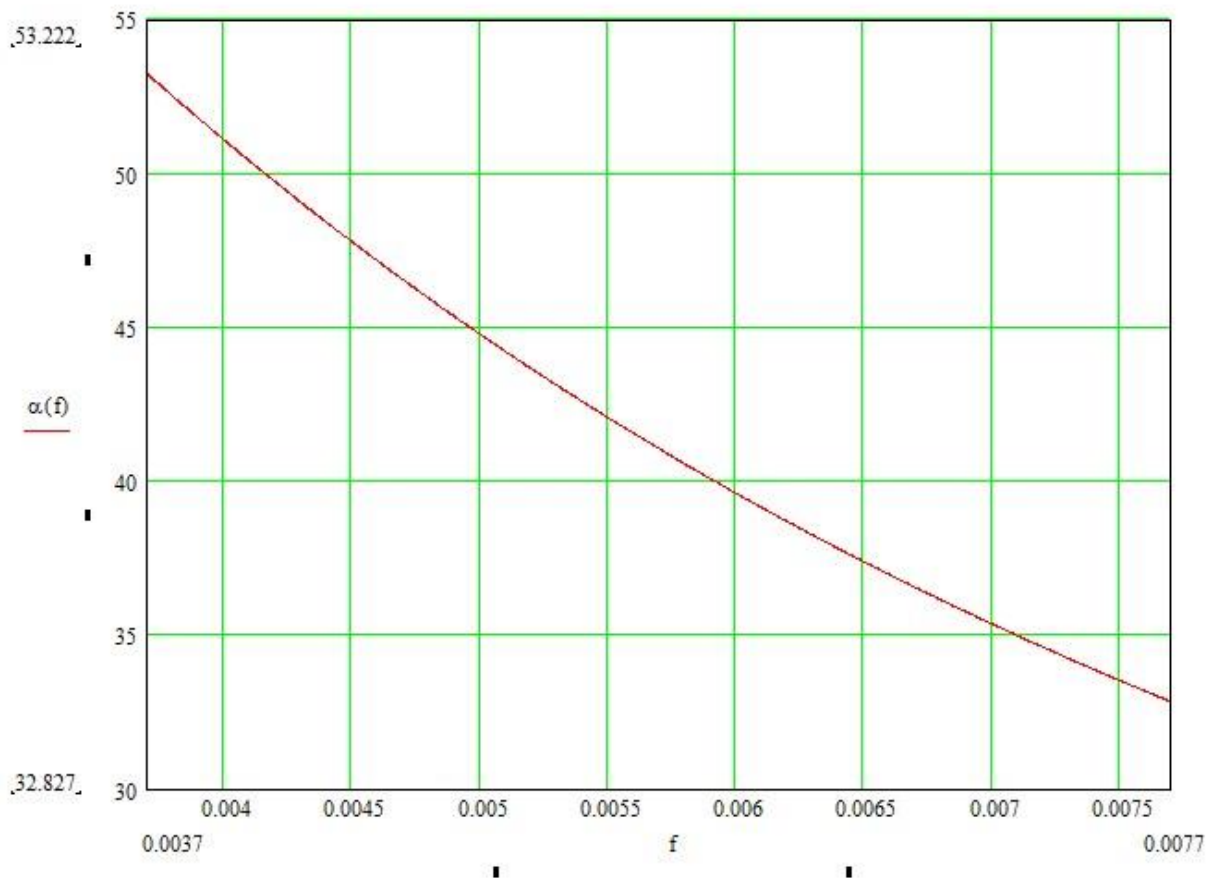


Рисунок 3.4 – Залежність кута поля зору відеокамери №3 від фокусної відстані

3.6.2 Дослідження можливостей тематичної обробки зображень відеокамер. У світі щорічно встановлюються мільйони камер спостереження, але все частіше при вивченні відеозаписів після тих чи інших інцидентів їх якість виявляється недостатньою для розпізнавання та ідентифікації людей або номерних знаків автомобілів, а це означає, що величезні кошти та ресурси були витрачені даремно.

Що спільного у погано спроектованої системи відеоспостереження та слабкого антивірусного пакета? Хибне почуття захищеності, що вони дають користувачеві. Хибне почуття безпеки змінюється розчаруванням після першого

інциденту. Щоб уникнути слабких місць, проектувальнику слід знати поширені помилки проектів відеоспостереження.

Якщо проект системи відеоспостереження потребує ідентифікації або розпізнавання людей, або потрібно ідентифікувати об'єкти - наприклад, номерні знаки, то потрібно не тільки отримати зображення поля огляду з достатньою роздільною здатністю, але й взяти до уваги такі фактори, як підсвічування, розташування камери і рух.

Порядок встановлення систем відеоспостереження

Як мінімум потрібно дотримуватися порядку установки для того, щоб надалі не виникало непередбачених ситуацій:

- Аналіз ризиків та оцінка ступеня кожного можливого ризику;
- Огляд об'єкта чи креслення об'єкта;
- Складання експлуатаційних вимог;
- Розробка проекту системи, що включає план місцевості чи план приміщення;
- Розробка плану тестування системи відеоспостереження;
- Установка системи та її передача замовнику;
- Документування результатів. Особливості вибору зони огляду

Багато рекомендацій виглядають продумано, наведемо найважливіші моменти, які потрібно враховувати під час планування зони огляду камери.

Чинники, які потрібно врахувати при виборі місця встановлення камери:

- Можлива поява іншої кількості листя на деревах в іншу пору року.
- Можлива поява сторонніх джерел світла.
- В залежності від часу доби та сезону сонячне світло може створювати відблиски або не забезпечувати достатніх умов освітлення.
- Вікна, будівлі, вода можуть викликати засвічення та погіршити якість зображення.
- Активність сцени – потрібно враховувати можливу появу тимчасових або нових об'єктів у зоні огляду камери.

- Якщо камера встановлюється для ідентифікації людей, її слід розмістити приблизно на висоті голови середнього зросту.

При виборі фокусної відстані об'єктива слід враховувати, що кут ясного зору людини по горизонталі становить приблизно 36° , що відповідає фокусній відстані $\sim 6,9$ мм (для відеокамери розміром матриці $1/3''$). Тому відеокамери з фокусною відстанню об'єктива менше $6,9$ мм візуально віддалятимуть зображення, понад $6,9$ мм – відповідно наближатимуть.

Фокусна відстань - це відстань між лінзою та матрицею відеокамери. Варто запам'ятати таке правило: чим менша фокусна відстань, тим більший кут огляду відеокамери і навпаки, чим більша фокусна відстань, тим менший кут огляду відеокамери. Фокусна відстань записується як $f = \dots \text{мм}$.

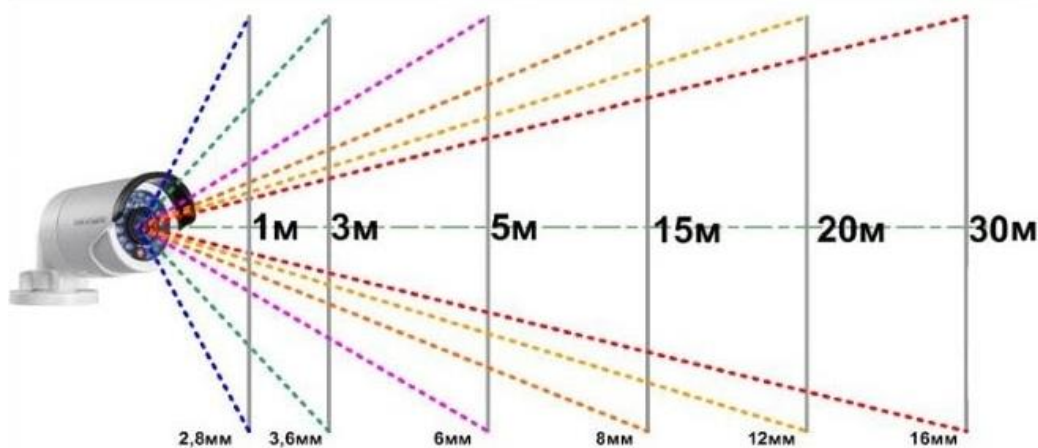


Рисунок 3.5 – Залежність відстані до об'єкта від фокусної відстані та кута огляду

З рисунка видно, що якщо потрібно мінімальною кількістю оглядових камер відеоспостереження стежити за периметром, варто встановити відеокамеру з малою фокусною відстанню і навпаки, якщо потрібна ідентифікація деталей: грошових купюр, автомобільних номерів, осіб, варто підбирати фокусну відстань об'єктива відеокамери з великим значенням.

Розрахунок дистанцій проводиться на основі вимог європейських норм для CCTV:

Лінійне розрізнення для виявлення об'єкта - 20 пікселів/м;

Лінійне розрізнення для розпізнавання - 100 пікселів/м;

Лінійне розрізнення для ідентифікації - 250 пікселів/м;

Кут огляду і фокусна відстань - це взаємопов'язані величини: зі збільшенням фокусної відстані - зменшується кут огляду, і навпаки. У той же час роздільна здатність камери буде впливати на деталізацію досить опосередковано.



Рисунок 3.6 – Зміна якості зображення при збільшенні фокусної відстані
Зони деталізації:

1. **Виявлення:** об'єкт займає від 25 до 30% висоти екрану. У цьому масштабі вирізняються характерні деталі об'єкта, наприклад, одяг.
2. **Розпізнавання:** об'єкт займає щонайменше 50% висоти екрану і можна сказати з високим ступенем вірогідності, чи спостерігався він раніше в зоні спостереження.

3. **Ідентифікація:** об'єкт займає щонайменше 100% висоти екрану, якість зображення і рівень деталізації достатні для однозначного встановлення особи.

Проведемо дослідження залежності відстані до об'єкта від роздільної здатності відеокамери для можливості проведення певних етапів тематичної обробки: виявлення, розпізнавання, ідентифікації.

Для проведення дослідження була вибрана відеокамера з діагоналлю матриці 1/2.8 дюйма, взята мінімальна фокусна відстань – 2.8мм.

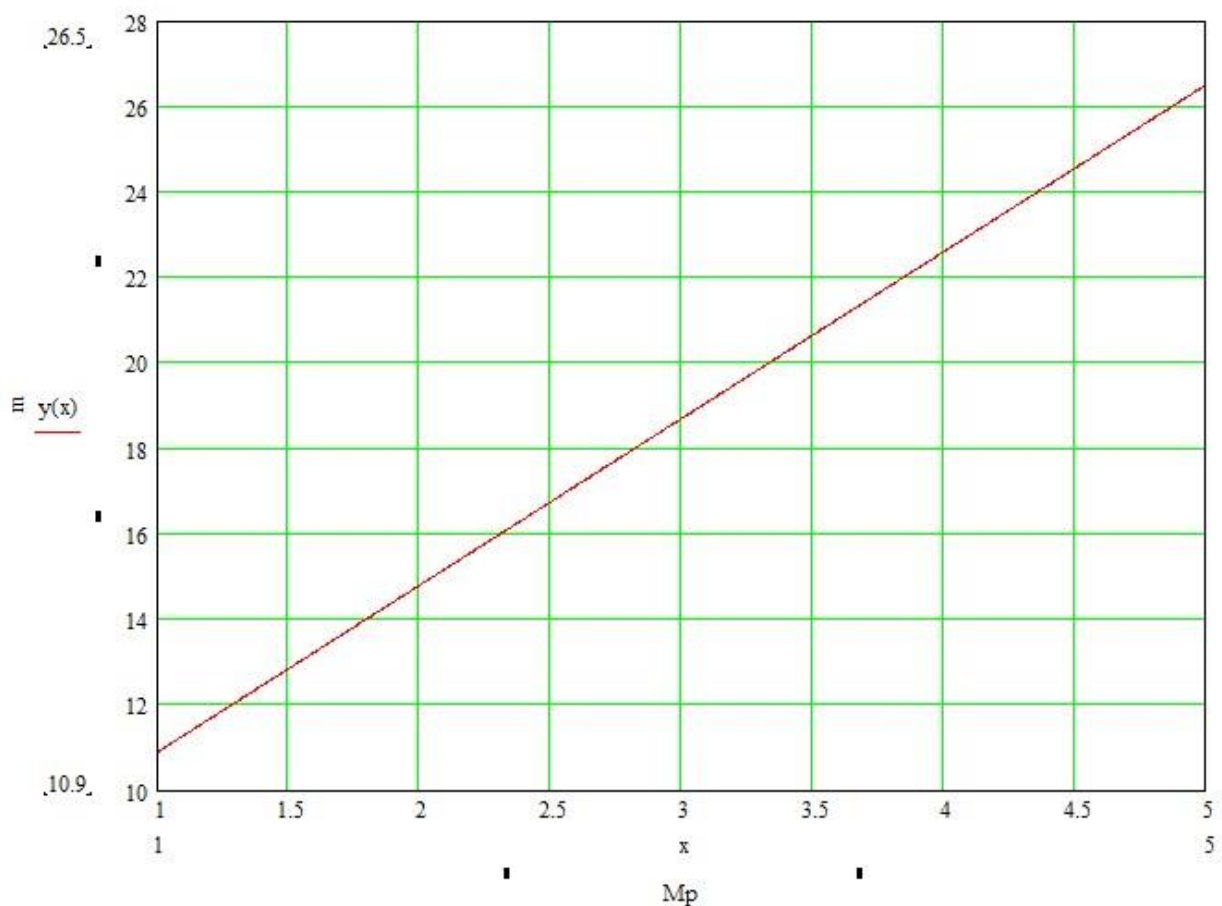


Рисунок 3.7 – Графік залежності відстані до об'єкта від роздільної здатності для можливості проведення виявлення об'єктів

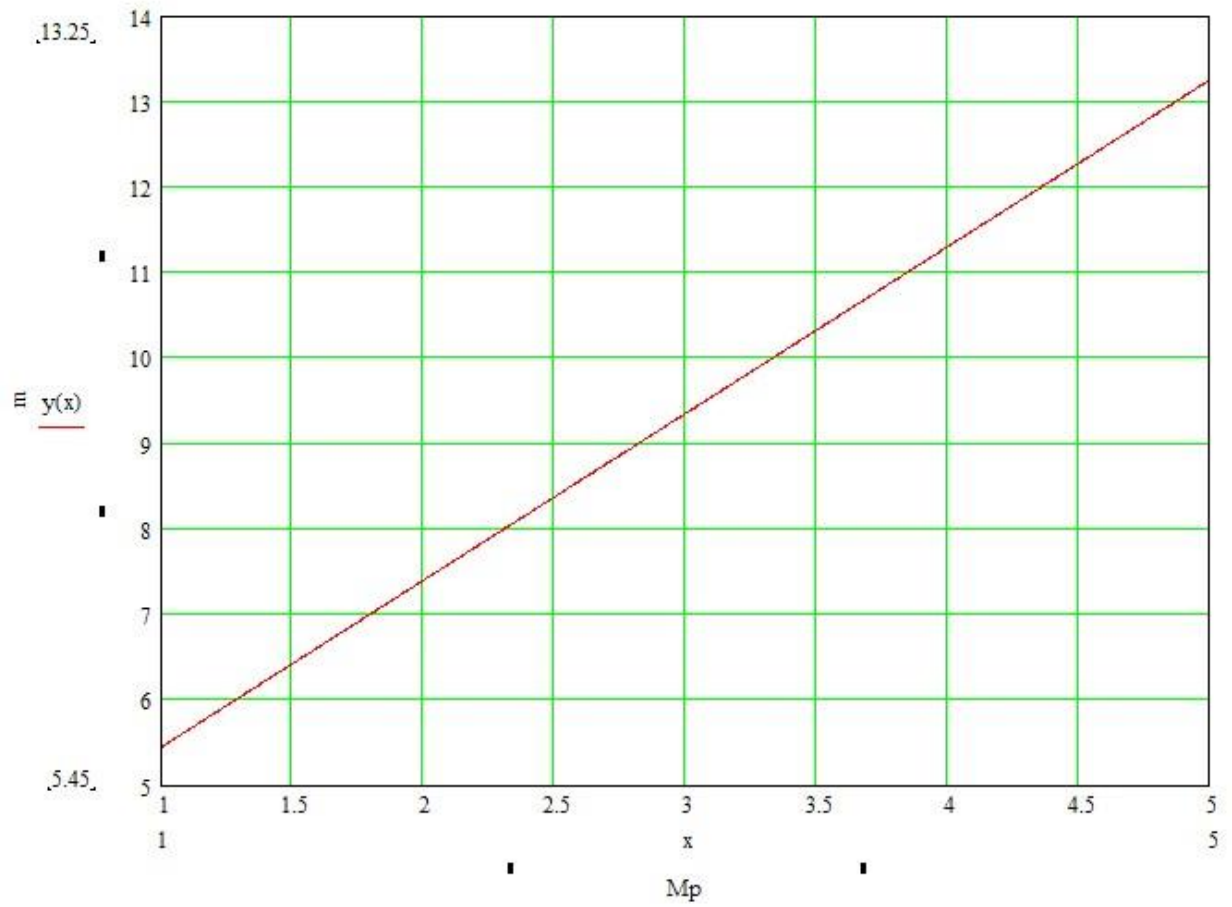


Рисунок 3.8 – Графік залежності відстані до об'єкта від роздільної здатності для можливості проведення розпізнавання об'єктів

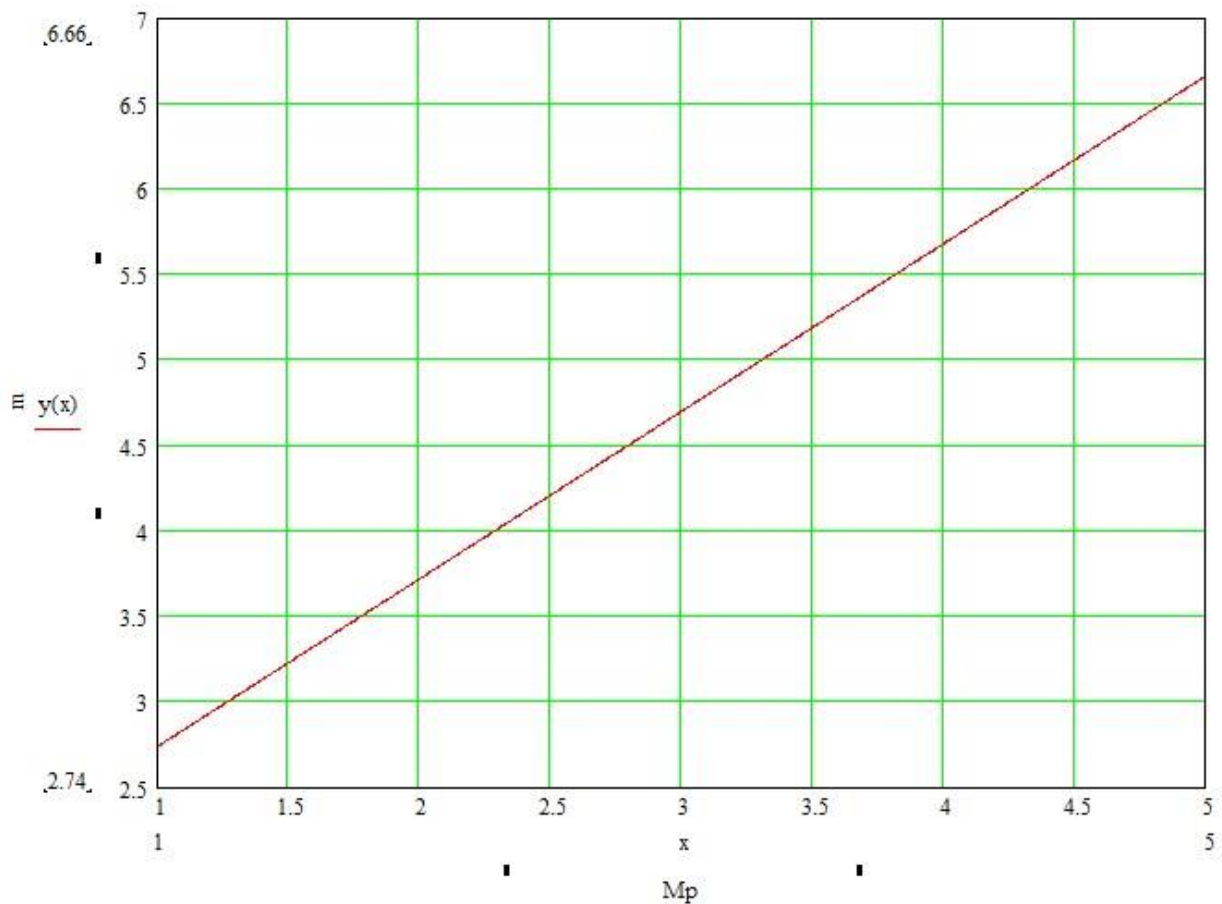


Рисунок 3.9 – Графік залежності відстані до об'єкта від роздільної здатності для можливості проведення ідентифікації об'єктів

З графіків можна зробити висновок, що:

- Зі збільшенням роздільної здатності збільшується дальність до об'єкта, на якій можливо проводити певну обробку зображень;
- Для роздільної здатності 5 Мп і фокусній відстані 2.8мм виявлення об'єктів можливо на відстані 26,2м, розпізнавання – 13,4м, ідентифікація – 6,7м.

Проведемо дослідження залежності відстані до об'єкта від фокусної відстані для можливості проведення певних етапів тематичної обробки: виявлення, розпізнавання, ідентифікації.

Для проведення дослідження була вибрана відеокамера з діагоналлю матриці 1/2.8 дюйма, роздільна здатність – 5 Мп.

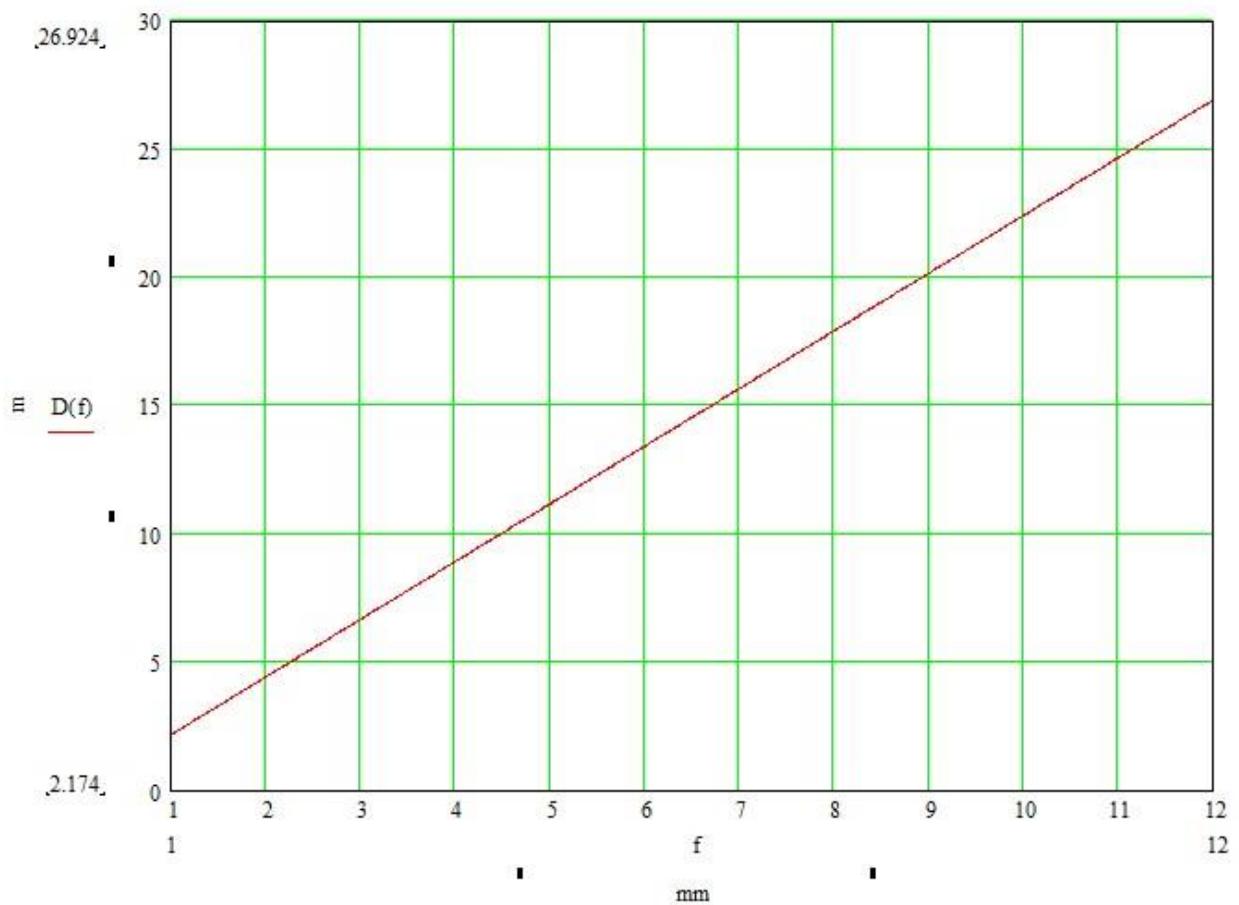


Рисунок 3.10 – Графік залежності відстані до об'єкта від фокусної відстані для можливості проведення ідентифікації об'єктів

З графіку можна зробити висновок, що:

- Зі збільшенням фокусної відстані збільшується дальність до об'єкта, на якій можливо проводити ідентифікацію об'єктів на зображеннях;
- Для фокусної відстані 12мм ідентифікація об'єктів (наприклад, впізнавання особистості людини) можливо на відстані 27м.

Таким чином, було проведено дослідження сучасної інтегрованої системи охорони об'єкта.

Проведено дослідження основних параметрів системи відеоспостереження для забезпечення виконання нею задач охорони. Показано, що для вирішення питань тематичної обробки зображень необхідно правильний вибір основних параметрів відеокамер, таких як роздільна здатність, кут поля зору, фокусна

відстань, а також правильне розміщення елементів системи відеоспостереження на об'єкті.

ВИСНОВКИ

Таким чином, у відповідності до поставленої мети в магістерській роботі було проведено дослідження особливостей функціонування інтегрованого апаратно-програмного комплексу системи безпеки об'єкту та можливості проведення тематичної обробки зображень системи відеоспостереження для забезпечення виконання завдань.

У першому розділі проведено аналіз комплексних систем безпеки спеціальних об'єктів. Розкрито принципи організації, структуру, склад, принцип дії інтегрованих систем безпеки. Показано, що тільки комплексна система охорони у складі систем відеоспостереження, охоронної та пожежної сигналізації, контролю управління доступу може забезпечити виконання завдань безпеки з необхідними показниками.

У другому розділі проведено аналіз інженерно-програмного комплексу технічних засобів систем безпеки об'єкту. Показано три основні складові комплексу: система контролю доступу, система охоронної сигналізації. Система відеоспостереження та відеоконтролю. Розкрито їх основні проектні рішення та принципи та порядок функціонування.

У третьому розділі проведено дослідження інтегрованого апаратно-програмного комплексу безпеки об'єкту. Проведено дослідження можливостей роботи програмно-апаратного комплексу побудови ІКБ, платформи ІКБ та програмного забезпечення. Для забезпечення можливості тематичної обробки зображень в цілях охорони об'єктів було проведено дослідження параметрів системи відеоспостереження та відеоконтролю по таким параметрам, як кут поля зору, роздільна здатність відеокамери для забезпечення можливості виявлення, розпізнавання та ідентифікації об'єктів на зображеннях.

Результати проведених досліджень можуть використовуватися під час проектування інтегрованої системи охорони об'єктів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мікропроцесорна техніка. Підручник / Ю.І. Якименко, Т.О. Терещенко, Є. І. Сокол, В.Я. Жуйкою, Ю.С. Петергеря; за ред. Т.О. Терещенка, 2-е видання, перероблене та доповнене. – К.: ІВЦ. Вид-во «Політехніка», «Кондор», 2008. – 594 с.
2. Волхонський В.В. Системи охоронної сигналізації: 2-е вид. Одеса: Екополіс і культура, 2005. 204 с.
3. Волковіцький В.Д., Волхонський В.В. цифрові системи ТВспостереження. Безпека, достовірність, інформація. Харків: 2009. С. 38-47.
4. Ворона В.А., Тихонов В.А. Системи контролю і управління доступом. Харків.: Гаряча лінія - Телеком, 2010. 272 с
5. Гедзберг Ю.М. Охоронне телебачення. К.: Гаряча лінія - Телеком, 2005. 312 с.
6. Двинских В.І. Аналіз вразливості системи охорони. оцінки показників уразливості. Офіційний сайт охоронно-інформаційного агентства Каскад-Сервіс. Харків: 2009. 78 с.
7. Крахмальов А.К. Перспективи розвитку інтегрованих системи безпеки. платформи інтеграції. Системи безпеки. Харків: 2010. с. 146-148.
8. Круглов Герман, Професійне відеоспостереження. Практика і технології аналогового і цифрового відеоспостереження, 2-е вид.: Пер. з англ. К.: Security Focus, 2010. - 640 с.
9. Кобилін О. А., Творошенко І.С. Методи цифрової обробки зображень: Навчальний посібник. Харків: ХНУРЕ. – 2021. – 124 с.
10. Волощук Ю.І. Сигнали та процеси у радіотехніці. Підручник для студентів вищих навчальних закладів у 4-х т.: ТОВ «Компанія СМІТ», 2005. – т. 4, 496 с.: іл.
11. Омелянчук А.М. Формування системи комплексної безпеки. Частина 2. Підготовка техзавдання і проектування. Системи безпеки. К.: 2009. С. 114-117.

12. Alessio S.M. Digital Signal Processing and Spectral Analysis for Scientists, 1-st Edition - Switzerland: Springer Cham, 2016. – 924p.

13. Синилов В. Г. Системи охоронної, пожежної та охоронно-пожежної сигналізації. Підручник для поч. проф. освіти. 5-е вид. К.: Видавничий центр «Академія» 2010. - 512 с.

ДОДАТОК А

Відеокамери з діагоналлю матриці 1/2.8 дюйма:

Фокусна відстань об'єктива, мм	Кут огляду, °		Зони деталізації, м								
	По горизонталі	По вертикалі	Спостереження			Впізнання			Ідентифікація		
			1Мп	2Мп	3Мп	1Мп	2Мп	3Мп	1Мп	2Мп	3Мп
2.8	90	58.7	10.5	15.7	18.3	5.24	7.86	9.14	2.62	3.93	4.57
3.6	75.8	47.3	13.5	20.2	23.5	6.74	10.1	11.8	3.37	5.06	5.88
3.8	72.8	45	14.2	21.3	24.8	7.12	10.7	12.4	3.56	5.34	6.2
4	70	43	15	22.5	26.1	7.49	11.2	13.1	3.75	5.62	6.53
5	58.5	35	18.7	28.1	32.6	9.36	14	16.3	4.68	7.02	8.16
6	50.1	29.4	22.5	33.7	39.2	11.2	16.9	19.6	5.62	8.43	9.79
8	38.6	22.3	30	44.9	52.2	15	22.5	26.1	7.49	11.2	13.1
10	31.3	17.9	37.5	56.2	65.3	18.7	28.1	32.6	9.36	14	16.3
12	26.3	15	44.9	67.4	78.3	22.5	33.7	39.2	11.2	16.9	19.6
16	19.9	11.2	59.9	89.9	104	30	44.9	52.2	15	22.5	26.1
50	6.41	3.61	187	281	326	93.6	140	163	46.8	70.2	81.6
60	5.35	3.01	225	337	392	112	169	196	56.2	84.3	97.9
90	3.57	2.01	337	506	588	169	253	294	84.3	126	147

